FortiOS™ Handbook

Getting Started for FortiOS 5.2

Getting Started for FortiOS 5.2

June 26, 2014

01-502-142188-20130423

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
June 26, 2014	Initial release.

Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

This guide explains how to get started with a FortiGate unit, as well as examining basic configuration tasks and best practices.

How this guide is organized

This guide contains the following sections:

- Differences between Models examines key types of differences between FortiGate models.
- Installation contains information about installing a FortiGate unit in your network.
- Using the Web-Based Manager describes the web-based manager and how to use it.
- Basic Administration contains information about basic tasks that should be done to set-up a new FortiGate unit.
- Next Steps contains a list resources that are available to help you with more advanced FortiGate configurations.

Differences between Models

This section examines some of the key types of differences that exist between different FortiGate models.

Features

There are certain features that are not available on all models. For example, the Switch Controller, which allows a FortiGate unit to manage a FortiSwitch unit, is only available on FortiGate models 100D, 140D, 200D, 240D, 600C, 800C, and 1000C.

Other features may be available only through the CLI on models, while other models have options in the web-based manager. For example, SSL content inspection is a CLI-only feature on FortiGate models 20C, 30C, and 40C, while models 60C+ have options in the web-based manager.

For more information about some of the features that vary by model, please see the *Feature/Platform Matrix*.

If there is a feature you believe your FortiGate model supports that does not appear in the web-based manager as expected, go to *System* > *Config* > *Features* and ensure the feature is turned on. For more information, see “Feature settings” on page 37.

Names

Naming conventions may vary between FortiGate models. For example, on some models the hardware switch interface used for the local area network is called *lan*, while on other units it is called *internal*.

Menus

Menus may vary by model. For example, on some FortiGate units, the main menu option *Router* is not available. Instead, routing is configured by going to *System* > *Network* > *Routing.*

Installation

This section provides information about how to install your FortiGate and use it in your network, after you have finished the initial set-up outlined in the FortiGate model's *QuickStart Guide*. The section also provides troubleshooting methods to use if the FortiGate does not function as desired after completing the installation.

The following topics are included in this section:

NAT/Route Mode vs Transparent Mode

A FortiGate unit can operate in one of two modes: NAT/Route or Transparent.

NAT/Route mode is the most common operating mode. In this mode, a FortiGate unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT). NAT/Route mode is also used when two or more Internet service providers (ISPs) will be used to provide the FortiGate with redundant Internet connections.

A FortiGate unit in Transparent mode is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiGate is added to a network in Transparent mode, no network changes are required, except to provide the FortiGate with a management IP address. Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.

Installing a FortiGate in NAT/Route Mode

There are two main types of FortiGate installations using NAT/Route mode: standard installations that receive Internet access from a single Internet service provider (ISP) and installations that have two or more ISPs for redundant Internet connections. For both installations, the first step is to decide if you want the FortiGate unit in switch or interface mode.

Switch Mode vs Interface Mode

In switch mode, all of the internal interfaces are part of the same subnet and treated as a single interface, which is called either *lan* or *internal* by default, depending on the FortiGate model. Switch mode is commonly used in settings where the network layout is fairly basic, with most users being on the same subnet.

In interface mode, the physical interfaces of the FortiGate unit are configured and handled individually, with each interface having its own IP address. Interfaces can be logically or virtually combined by configuring them as part of either hardware or software switches, which allow multiple interfaces to be treated as a single interface. FortiGate units that are in interface mode by default start with a hardware switch called either *lan* or *internal,* depending on the FortiGate

model. This mode is designed for complex networks where different subnets are used to compartmentalize the network traffic.

The default mode that a FortiGate starts in varies depending on the model. Switch mode has been the most common factory default setting; however, the number of models that have interface mode as their default setting is increasing.

In order to determine which mode your FortiGate unit is in, go to *System* > *Network* > *Interfaces.* Locate the interface called either *lan* or *internal*, which all FortiGate units have be default. If the interface is listed as a physical interface in the *Type* column, then your FortiGate is in switch mode. If the interface is a hardware switch, then your FortiGate is in interface mode.

You can also determine what mode your FortiGate is by going to *System* > *Dashboard* > *Status* and enter either of the following commands into the *CLI Console*: `config system global show`. In the output that is displayed after you hit the Enter key, find the line that begins with `set internet-switch-mode`. This will tell you which mode your FortiGate is currently in.

If you need to change the mode your FortiGate unit is in, go to *System* > *Dashboard* > *Status* and enter either of the following commands into the *CLI Console*:

Before switching modes, you must make sure that none of the physical ports that make up the *lan* or *internal* interface are referenced in the FortiGate configuration.

1. Command to change the FortiGate to switch mode:

```
config system global
  set internet-switch-mode switch
end
```

2. Command to change the FortiGate to interface mode:

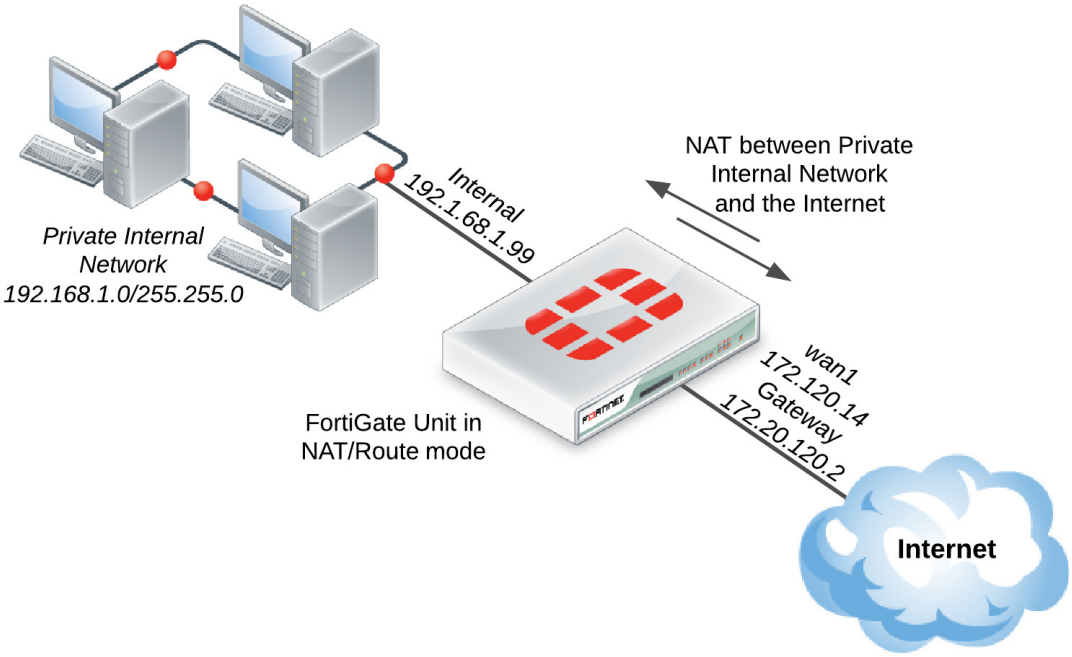
```
config system global
  set internet-switch-mode interface
end
```

There is a third mode, called hub mode, that is available on some FortiGate models. Hub mode is similar to switch mode, except the network device that it is emulating is a Layer 2 device instead of Layer 3. In hub mode, he interfaces do not learn the MAC addresses of the devices on the network they are connected to and may also respond quicker to network changes in some circumstances.

You should only select hub mode if you are having network performance issues when operating with switch mode. The configuration of the FortiGate unit is the same whether in switch mode or hub mode.

Standard Installation in NAT/Route Mode

Figure 1: Network with a FortiGate unit in NAT/Route mode and a single ISP



1. Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment.
2. Connect a PC to the FortiGate using an internal port (typically port 1).
3. Power on the ISP's equipment, the FortiGate unit, and the PC on the internal network.
4. From the PC on the internal network, connect to the FortiGate's web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models *QuickStart Guide*). Login using an admin account (the default admin account has the username `admin` and no password).
5. Go to *System* > *Network* > *Interfaces* and edit the Internet-facing interface. Set *Addressing Mode* to *Manual* and the *IP/Netmask* to your public IP address. Select *OK*.
6. Edit the internal interface. Set *Addressing Mode* to *Manual* and set the *IP/Netmask* to the private IP address you wish to use for the FortiGate. Select *OK*.
7. Go to *Router* > *Static* > *Static Routes* (or *System* > *Network* > *Routing*, depending on your FortiGate model) and select *Create New* to add a default route. Set the *Destination IP/Mask* to 0.0.0.0/0.0.0.0, the *Device* to the Internet-facing interface, and the *Gateway* to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements. Select *OK*.

A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can either edit it or delete it and add a new one.

8. (Optional) The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to *System* > *Network* > *DNS* and add *Primary* and *Secondary* DNS servers. Select *Apply*.

9. If your network uses IPv4 addresses, go to *Policy & Objects* > *Policy* > *IPv4* and select *Create New* to add a security policy that allows users on the private network to access the Internet.

Some FortiGate models include the IPv4 security policy in the default configuration. If you have one of these models, this step has already been done for you and as soon as your FortiGate unit is connected and the computers on your internal network are configured, users should be able to access the Internet.

If your network uses IPv6 addresses, go to *Policy & Objects* > *Policy* > *IPv6* and select *Create New* to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to *System* > *Config* > *Features*, turn on *IPv6*, and select *Apply*. For more information on IPv6 networks, see the *IPv6 Handbook*.

In the policy, set the *Incoming Interface* to the internal interface and the *Outgoing Interface* to the Internet-facing interface. You will also need to set *Source Address*, *Destination Address*, *Schedule*, and *Service* according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.

Make sure the *Action* is set to *ACCEPT*. Turn on *NAT* and make sure *Use Destination Interface Address* is selected. Select *OK*.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the *Security Profiles* handbook.

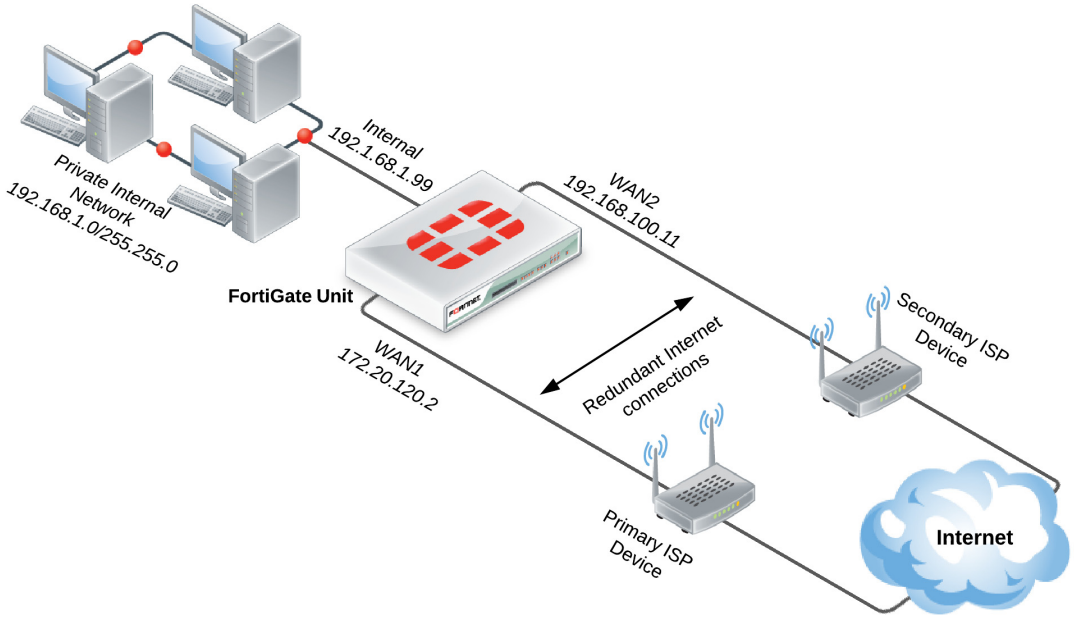
Results

Users on the internal network are now able to browse the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

Redundant Internet Installation in NAT/Route Mode

If you have previously configured your FortiGate using the standard installation, you will have to delete all routes and policies that refer to an interface that will be used to provide redundant Internet. This includes the default Internet access policy that is included on many FortiGate models.

Figure 2: Network with a FortiGate unit in NAT/Route mode using redundant Internet



1. Connect the FortiGate's Internet-facing interfaces (typically WAN1 and WAN2) to your ISP-supplied equipment.
2. Go to *System* > *Network* > *Interfaces* and select *Create New* > *Virtual WAN*. This will create a virtual WAN link, which is used to group multiple Internet connections together so that the FortiGate unit can treat them as a single interface.
3. Select an appropriate method of *WAN Load Balancing* from the following options:
   - *Source IP based* - The next hop is based on the traffic's source IP address.
   - *Weighted Round Robin* - Weight is input for all the active members of the WAN link.
   - *Spill-over* - A traffic cap is defined for active members; when it is exceeded, the traffic will automatically activate the standby link.
   - *Source-Destination IP based* - The next hop is based on both the traffic's source and destination IP address.
   - *Measured-Volume based* - A volume ratio is set for each active member of the WAN link.
4. Add your Internet-facing interfaces to the virtual WAN link, configuring load balancing as required for each interface.
5. Go to *Router* > *Static* > *Static Routes* and create a new default route. Set *Device* to the virtual WAN link.

6. If your network uses IPv4 addresses, go to *Policy & Objects* > *Policy* > *IPv4* and select *Create New* to add a security policy that allows users on the private network to access the Internet.

   If your network uses IPv6 addresses, go to *Policy & Objects* > *Policy* > *IPv6* and select *Create New* to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to *System* > *Config* > *Features*, turn on *IPv6*, and select *Apply*. For more information on IPv6 networks, see the *IPv6 Handbook*.

   In the policy, set the *Incoming Interface* to the internal interface and the *Outgoing Interface* to the virtual WAN link. You will also need to set *Source Address*, *Destination Address*, *Schedule*, and *Service* according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.

   Make sure the *Action* is set to *ACCEPT*. Turn on *NAT* and make sure *Use Destination Interface Address* is selected. Select *OK*.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the *Security Profiles* handbook.

Results

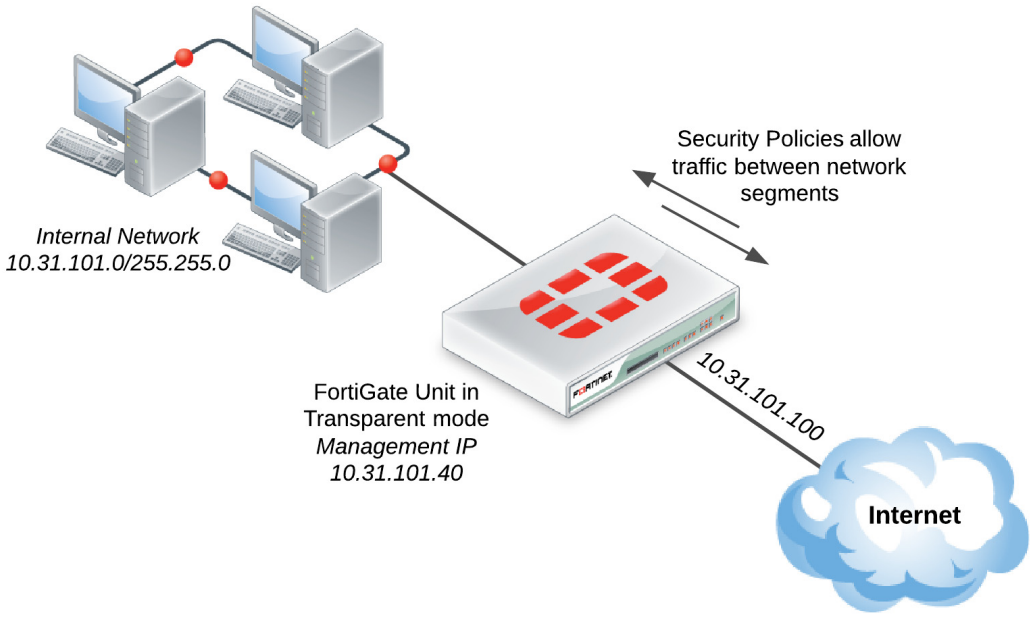
Users on the internal network are now able to browse the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

The amount of traffic will use an individual member of the virtual WAN link will depend on the load balancing method you selected. You can view this usage by going to *System* > *FortiView* > *All Sessions* and viewing the *Dst Interface* column. If this column is not shown, right-click on the title row and select *Dst Interface* from the dropdown menu. Scroll to the bottom of the menu and select *Apply*.

Installing a FortiGate in Transparent Mode

Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the *System Information* widget, found at *System* > *Dashboard* > *Status*.

Figure 3: Network with a FortiGate unit in Transparent mode



1. Before connecting the FortiGate unit to your network, go to *System* > *Dashboard* > *Status* and locate the *System Information* widget. Beside *Operation Mode*, select *Change*.
2. Set the *Operation Mode* to *Transparent*. Set the *Management IP/Netmask* and *Default Gateway* to connect the FortiGate unit to the internal network. Select *OK*.
3. Access the web-based manager by browsing to the new management IP.
4. (Optional) The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to *System* > *Network* > *DNS* and add *Primary* and *Secondary* DNS servers. Select *Apply*.
5. If your network uses IPv4 addresses, go to *Policy & Objects* > *Policy* > *IPv4* and select *Create New* to add a security policy that allows users on the private network to access the Internet.

   If your network uses IPv6 addresses, go to *Policy & Objects* > *Policy* > *IPv6* and select *Create New* to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to *System* > *Config* > *Features*, turn on *IPv6*, and select *Apply*. For more information on IPv6 networks, see the *IPv6 Handbook*.

   Set the *Incoming Interface* to the internal interface and the *Outgoing Interface* to the Internet-facing interface (typically WAN1). You will also need to set *Source Address*, *Destination Address*, *Schedule*, and *Service* according to your network requirements. You

can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified.

Make sure the *Action* is set to *ACCEPT*. Select *OK*.

It is recommended to avoid using any security profiles, such as AntiVirus or web filtering, until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

For more information about using security profiles, see the *Security Profiles* handbook.

6. Go to *System* > *Dashboard* > *Status* and locate the *System Resources* widget. Select *Shutdown* to power off the FortiGate unit.

   Alternatively, you can also use the CLI command `execute shutdown`.
7. Connect the FortiGate unit between the internal network and the router.
8. Connect the Internet-facing interface to the router's internal interface and connect the internal network to the FortiGate using an internal port (typically port 1).
9. Power on the FortiGate unit. You will experience downtime before the FortiGate unit starts up completely.

Results

Users on the internal network are now able to browse to the Internet. They should also be able to connect to the Internet using any other protocol or connection method that you defined in the security policy.

If a FortiGate unit operating in Transparent mode is installed between your internet network and a server that is providing a network service to the internal network, such as DNS or DHCP, you must add a wan1-to-internal policy to allow the server's response to flow through the FortiGate unit and reach the internal network.

Troubleshooting your FortiGate Installation

If your FortiGate does not function as desired after completing the installation, try the following troubleshooting methods (those methods that are only applicable to one transparent mode are marked):

1. **Use FortiExplorer if you can't connect to the FortiGate over Ethernet.**

   If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's *QuickStart Guide* for details.
2. **Check for equipment issues.**

   Verify that all network equipment is powered on and operating as expected. Refer to the *QuickStart Guide* for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate unit LED indicators.
3. **Check the physical network connections.**

   Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device.

   Also, check the *Unit Operation* widget, found at *System* > *Dashboard* > *Status*, to make sure the ports used in the connections are shown in green.

4. **Verify that you can connect to the internal IP address of the FortiGate unit (NAT/Route mode).**

   Connect to the web-based manager from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.

   If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the web-based manager, check the settings for administrative access on that interface.

5. **Verify that you can connect to the management IP address of the FortiGate unit (Transparent mode).**

   From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

6. **Check the FortiGate interface configurations (NAT/Route mode).**

   Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure *Addressing Mode* is set to the correct mode.

7. **Verify the security policy configuration.**

   Go to *Policy & Objects* > *Policy* > *IPv4* or *Policy & Objects* > *Policy* > *IPv6* and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the *Sessions* column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select *Sessions*, and select *Apply*).

   If you are using NAT/Route mode, check the configuration of the policy to make sure that *NAT* is turned on and that *Use Destination Interface Address* is selected.

8. **Verify that you can connect to the Internet-facing interface's IP address (NAT/Route mode).**

   Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate unit is not allowing sessions from the internal interface to Internet-facing interface.

9. **Verify the static routing configuration (NAT/Route mode).**

   Go to *Router* > *Static* > *Static Routes* or *System* > *Network* > *Routing* and verify that the default route is correct. View the Routing Monitor (found either on the same page or at *Router* > *Monitor* > *Routing Monitor*) and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as *Connected*, one for each connected FortiGate interface.

10. **Verify that you can connect to the gateway provided by your ISP.**

    Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.

11. **Verify that you can communicate from the FortiGate unit to the Internet.**

    Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

12. **Verify the DNS configurations of the FortiGate unit and the PCs.**

    Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`

    If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

13. Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, you should confirm that it can reach the FortiGuard network.

First, check the *License Information* widget to make sure that the status of all FortiGuard services matches the services that you have purchased.

Go to *System* > *Config* > *FortiGuard*. Expand *Web Filtering and Email Filtering Options* and select *Test Availability*. After a minute, the web-based manager should indicate a successful connection.

14. Consider changing the MAC address of your external interface (NAT/Route mode).

Some ISPs do not want the MAC address of the device connecting to their network cable to change. If you have added a FortiGate unit to your network, you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
  edit <interface>
    set macaddr <xx:xx:xx:xx:xx:xx>
  end
end
```

15. Check the FortiGate bridge table (Transparent mode).

When the FortiGate is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit.

Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed that is a likely cause. Check for the MAC address of the interface or device in question.

To list the existing bridge instances on the FortiGate unit, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. This could indicate that the device is either not connected or not operating. Check the device's network connections and make sure they are connected and operational.

16. **Either reset the FortiGate unit to factory defaults or contact the technical assistance center.**

    If all else fails, reset the FortiGate unit to factory defaults using the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.

You can also contact the technical assistance center. For contact information, go to support.fortinet.com.

Using the Web-Based Manager

This section contains an introduction to the web-based manager administrative interface (sometimes referred to as a graphical user interface, or GUI) of your FortiGate unit and the information you can access from the various dashboards and tables.

The following topics are included in this section:

Connecting to the web-based manager

After you have completed the initial installation for your FortiGate unit, there are two ways to connect to the web-based manager: using FortiExplorer or a web browser.

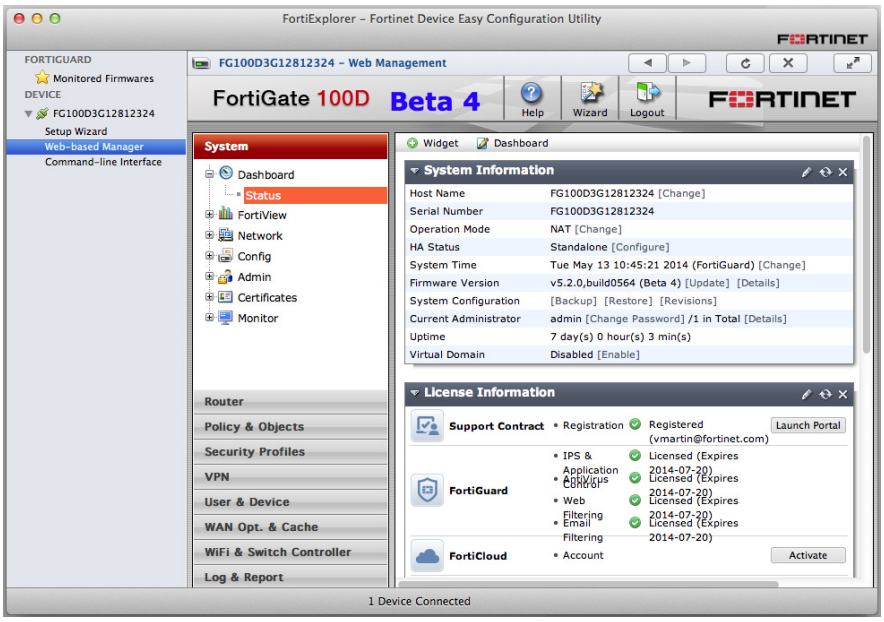
FortiExplorer

To connect to the web-based manager using FortiExplorer, connect your management computer to your FortiGate unit's USB MGMT port, using the cable that came with the unit. FortiExplorer should open automatically once the devices are connected; if it does not, open the program manually.

To connect to the web-based manager, go to *Devices* > *Web-based Manager* and enter your username and password. If you have not changed the admin account's password, use the default username, `admin`, and leave the password field blank.

The web-based manager will now be displayed in FortiExplorer.

Figure 4: Connecting to the web-based manager with FortiExplorer



Web browser

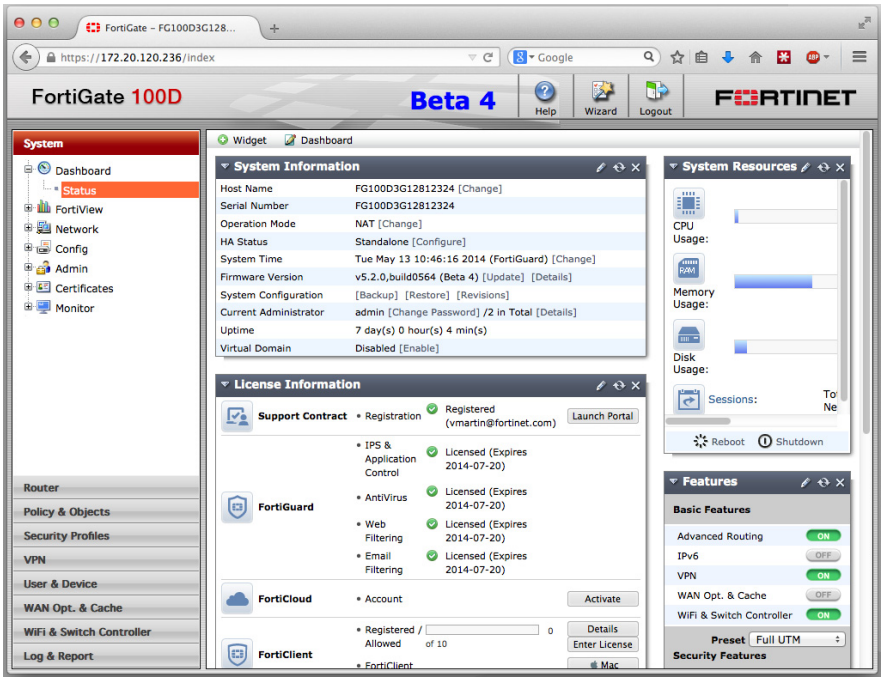
The recommended minimum screen resolution for properly displaying the web-based manager is 1280 by 1024. Check the *FortiOS Release Notes* for information about browser compatibility.

In order to connect to the web-based manager using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. By default, an interface has already been set up that allows HTTPS access, with the IP address 192.168.1.99.

Browse to https://192.168.1.99 and enter your username and password. If you have not changed the admin account's password, use the default username, `admin`, and leave the password field blank.

The web-based manager will now be displayed in your browser.

Figure 5: Connecting to the web-based manager with a web browser (Firefox)



If you wish to use a different interface to access the web-based manager, do the following:

1. Go to *System* > *Network* > *Interfaces* and edit the interface you wish to use for access. Take note of its assigned IP address.
2. Beside *Administrative Access*, select *HTTPS*. You can also select *HTTP*, although this is not recommended as the connection will be less secure.
3. Select *OK*.
4. Browse to the IP address using your chosen protocol.

The web-based manager will now be displayed in your browser.

Menus

Some menus may not initially appear on your FortiGate, while others only appear on certain FortiGate models or when certain features/modes are enabled. If there is a menu you believe your FortiGate model supports that does not appear in the web-based manager as expected, go to *System* > *Config* > *Features* and ensure the feature is turned on. For more information, see "Feature settings" on page 37.

The web-based manager contains the following main menus, which provide access to configuration options for most of the FortiOS features:

System	Configure system settings, such as network interfaces, virtual domains (VDOMs), DNS services, administrators, certificates, High Availability (HA), system time, set system options, and set display options on the web-based manager. The *System* menu also contains the Status and FortiView dashboards. For more information, see "Dashboards" on page 24.
Router	Configure static, dynamic and multicast routing and view the router monitor. On certain FortiGate models, routing is configured by going to *System* > *Network* > *Routing*.
Policy & Objects	Configure firewall policies, protocol options, the Central NAT Table, and supporting content for policies including scheduling, services, traffic shapers, addresses, virtual IP and load balancing.
Security Profiles	Configure antivirus and email filtering, web filtering, intrusion protection, data leak prevention, application control, VOIP, ICAP and Client Reputation.
VPN	Configure IPsec and SSL virtual private networking.
User & Device	Configure user accounts and user authentication including external authentication servers.This menu also includes endpoint security features, such as FortiClient configuration and application detection patterns.
WAN Opt. & Cache	Configure WAN optimization and web caching to improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers.
WiFi Controller	Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. On certain FortiGate models, this menu is called *WiFi & Switch Controller* and has additional features allowing for FortiSwitch units to be managed by the FortiGate.
Log & Report	Configure logging and alert email as well as reports. View log messages and reports.
Current VDOM	This menu only appears when VDOMs are enabled on the unit and is used to switch between VDOMs.

Dashboards

The various dashboard menus provides a way to access information about network activity and events, as well as configure basic system settings.

There are two main dashboards: the Status Dashboard and the FortiView Dashboards.

Status Dashboard

The *Status Dashboard* can be found by going to *System* > *Dashboard* > *Status*. The dashboard consists of a number of widgets, each displaying a different set of information. A number of pre-configured widgets are available which can be customized to meet your needs.

To choose which widgets will be shown, select *Widget* and select the widget you wish to view, which will add it to the dashboard. Widgets can be rearranged in the *Status Dashboard* for easier access and viewing. You can also change the display from two columns to one by selecting the *Dashboard* button, selecting *Edit Dashboard* and choosing the one column display from the options.

Custom Dashboards

You can create custom dashboards that will be added to the menu under the default *Status Dashboard*. You can add, remove, or rename a dashboard, regardless of whether it is default. You can also reset the Dashboard menu to its default settings by selecting *Reset Dashboards*.

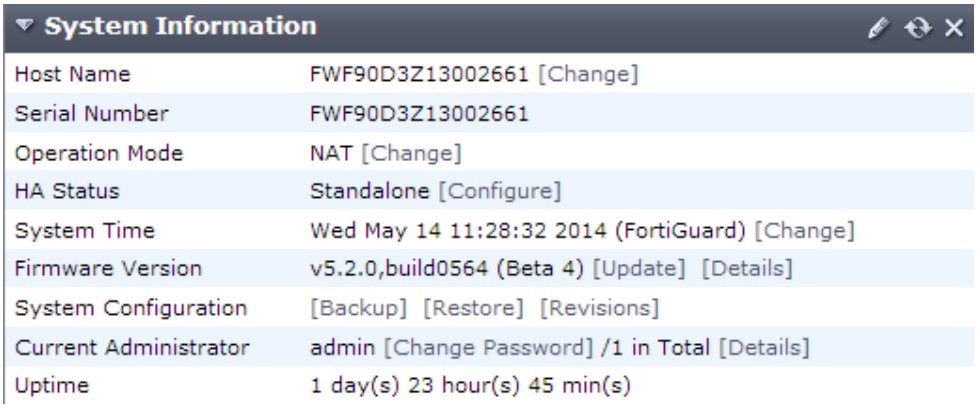
If VDOMs are enabled, only the dashboards within Global are available for configuration.

To add a dashboard

1. Go to *System* > *Dashboard* > *Status*.
2. Select *Dashboard*, located at the top left of the page.
3. Select *Add Dashboard*.

System Information

Figure 6: The *System Information* widget



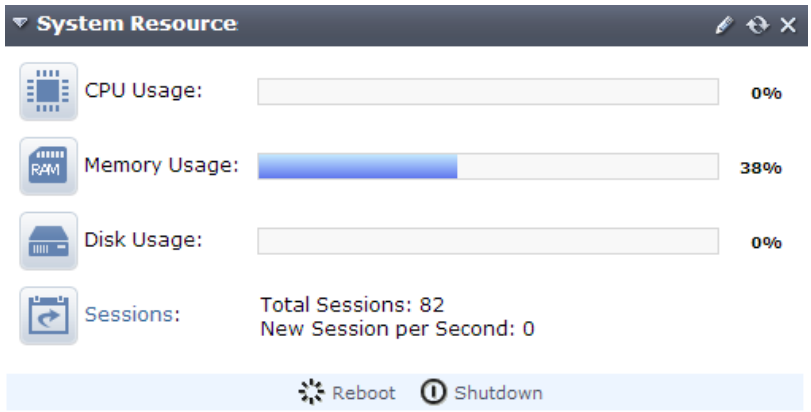
The *System Information* widget shows status information on the FortiGate unit. Some configuration details/modes can be changed through the widget.

Host Name	The name of the FortiGate unit. If the FortiGate unit is in HA mode, this information is not displayed.
Serial Number	The serial number of the FortiGate unit. The serial number is specific to that FortiGate unit and does not change with firmware upgrades.
Operation Mode	The current operating mode of the FortiGate unit (a FortiGate unit can operate in NAT mode or Transparent mode). If virtual domains are enabled, this field shows the operating mode of the current virtual domain. The Global System Status dashboard does not include this information.
HA Status	The status of High Availability (HA) within the cluster. Standalone indicates the FortiGate unit is not operating in HA mode. Active-Passive or Active-Active indicate the FortiGate unit is operating in HA mode. Select *Configure*, to change the HA configuration.
Cluster Name	The name of the HA cluster for this FortiGate unit. The FortiGate unit must be operating in HA mode to display this field.
Cluster Members	The FortiGate units in the HA cluster. Information displayed about each member includes host name, serial number, and whether the FortiGate unit is a primary (master) or subordinate (slave) FortiGate unit in the cluster. The FortiGate unit must be operating in HA mode with virtual domains disabled to display this information.
Virtual Cluster 1 **Virtual Cluster 2**	The role of each FortiGate unit in virtual cluster 1 and virtual cluster 2. The FortiGate unit must be operating in HA mode with virtual domains enabled to display this information.
System Time	The current date and time.
Firmware Version	The version of the current firmware installed on the FortiGate unit.

System Configuration	The time period of when the configuration file was backed up.
Current Administrator	The number of administrators currently logged into the FortiGate unit. Select *Details* to view more information about each administrator that is currently logged in
Uptime	The time in days, hours, and minutes since the FortiGate unit was started or rebooted.
Virtual Domain	Status of virtual domains on your FortiGate unit. This information will only appear when VDOMs have been enabled.
Explicit Proxy Load Balance	The status of each feature. Select *Enable* or *Disable* to change the status of the feature. When enabled, the menu option appears. This information will only appear when redundant Internet connections are enabled.

System Resources

Figure 7: The *System Resources* widget



The *System Resources* widget displays basic FortiGate unit resource usage. This widget displays the information for CPU and memory in either real-time or historical data. For FortiGate units with multiple CPUs, you can view the CPU usage as an average of all CPUs or each one individually.

This widget also is where you reboot or shutdown the FortiGate unit.

The options to reboot or shutdown the FortiGate unit are not available for an admin using the *prof_admin* profile.

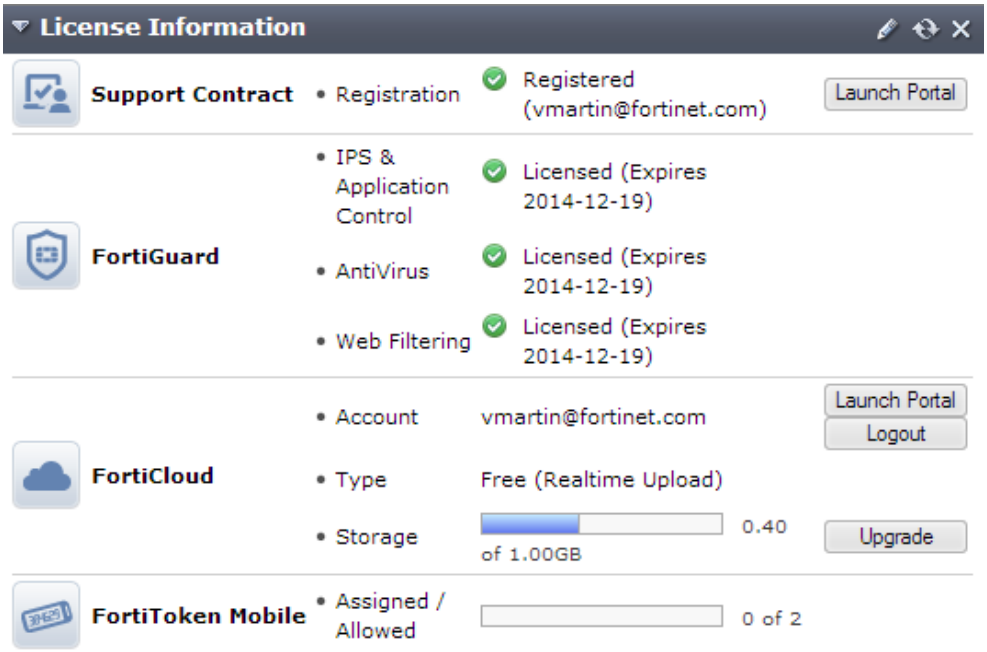
USB Modem

Figure 8: The *USB modem* widget

The *USB modem* widget enables you to monitor the status of your USB modem and configure it as needed.

License Information

Figure 9: The *License Information* widget



The *License Information* widget displays the status of your technical support contract, FortiGuard subscriptions, FortiCloud account, and other licenses.

When a new FortiGate unit is powered on, it automatically searches for FortiGuard services. If the FortiGate unit is configured for central management, it will look for FortiGuard services on the configured FortiManager system. The FortiGate unit sends its serial number to the FortiGuard service provider, which then determines whether the FortiGate unit is registered and has valid contracts for FortiGuard subscriptions and FortiCare support services. If the FortiGate unit is registered and has a valid contract, the *License Information* is updated.

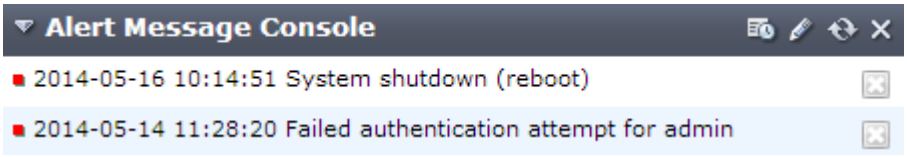
When a license is near to its expiry date, an option to extend it will appear that allows you to add a new license as soon as you buy it.

Support Contract	Displays details about your current Fortinet Support contract. • If *Not Registered* appears, select *Register* to register the FortiGate unit. • If *Expired* appears, select *Renew* for information on renewing your technical support contract. Contact your local reseller. • If *Registered* appears, the name of the support that registered this FortiGate unit is also displayed. The various types of contracts that you currently have and the expiry date for each type. • You can select *Launch Portal* to log into the Fortinet Support account that registered this FortiGate unit.
FortiGuard Services	Displays your current licenses for services from FortiGuard. Select *Extend* or *Renew* to update any of the licenses (these options only appear when a license is expired or close to expiry).

FortiCloud	Displays details about your current FortiCloud subscription. If the green *Activate* button appears, select it to either create a new account or add the FortiGate unit to an existing account. If you have already activated FortiCloud, the name of the *Account* will be listed. Select *Launch Portal* to view your FortiCloud account in a web browser. Information on the current *Type* and *Storage* is also listed. You can select *Upgrade* to change the type of your FortiCloud account.
FortiClient Software	Displays FortiClient license details and the number of *Register* and *Allowed* FortiClient users. You can select *Details* for more information about the current FortiClient users. This information will only appear when you have a FortiClient license.
FortiToken Mobile	Displays the number of *Assigned* and *Allowed* FortiTokens.
SMS	Displays the number of *Sent* and *Allowed* SMS messages. You can select *Add Messages* to configure a new SMS message. This information will only appear when SMS has been configured.
Virtual Domain	Displays the maximum number of virtual domains the FortiGate unit supports with the current license. For some FortiGate models, you can select the *Purchase More* link to purchase a license key through Fortinet technical support to increase the maximum number of VDOMs.

Alert Message Console

Figure 10: The *Alert Messages Console* widget



The *Alert Messages Console* widget helps you monitor system events on your FortiGate unit such as firmware changes, network security events, or virus detection events. Each message shows the date and time that the event occurred.

You can configure the alert message console settings to control what types of messages are displayed on the console.

To configure the Alert Message Console

1. Locate the *Alert Message Console* widget within the Dashboard menu.
2. Select the *Edit* icon in the *Alert Message Console* title bar.
3. Select the types of alerts that you do not want to be displayed in the widget.
4. Select *OK*.

Advanced Threat Protection Statistics

Figure 11: The *Advanced Threat Protection Statistics* widget

Advanced Threat Protection Statistics

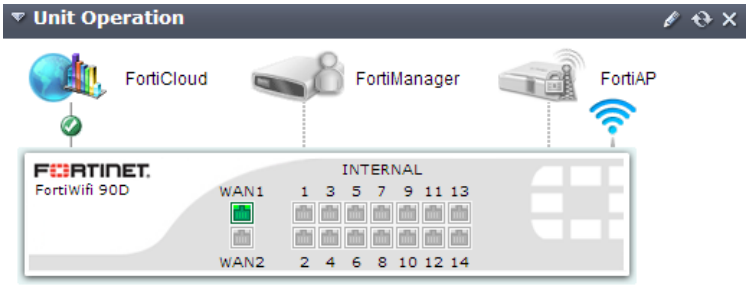
FortiGate Statistics	
Number of Files Scanned	430682
Malicious	1
Detected Zero-Day Malware Variants	0
Suspicious Files	0
Clean	430681

FortiGuard Sandbox Statistics (Last 7 Days)	
# of Files Submitted to FortiGuard Sandbox	0
Malicious	0
Clean	0

The *Advanced Threat Protection Statistics* widget displays a count of detected malware and files scanned for these types of intrusions. It also displays statics on the number of files sent to FortiGuard Sandbox and the results from sandboxing.

Unit Operation

Figure 12: The *Unit Operation* widget

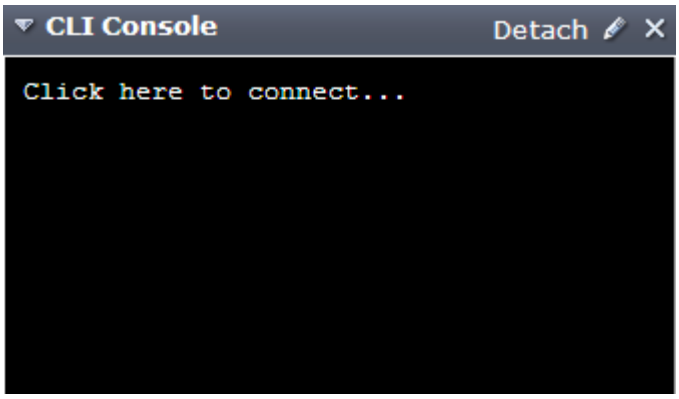


The *Unit Operation* widget is an illustrated version of the FortiGate unit's front panel that shows the status of the FortiGate unit's network interfaces. Interfaces appears green when connected. Hover the mouse pointer over an interface to view further details.

Icons around the front panel indicate when the FortiGate unit is connected to a FortiAnalyzer or FortiManager device, or FortiClient installations. Select the icon in the widget to jump to the configuration page for each device. When connected to one of these devices, a green check mark icon appears next to the icon. If the device communication is configured but the device is unreachable, a red X appears.

CLI Console

Figure 13: The *CLI Console* widget



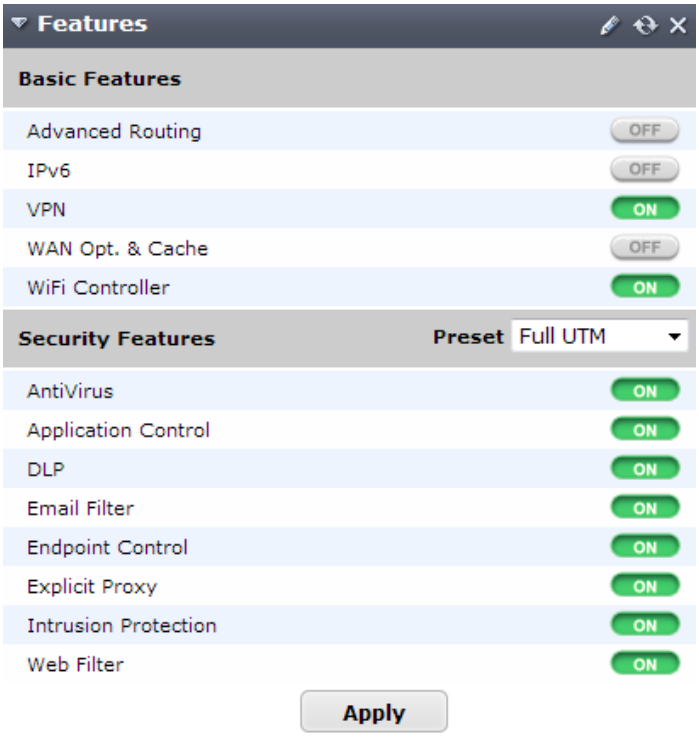
The *CLI Console* widget enables you to access the CLI without exiting from the web-based manager.

The two controls located on the CLI Console widget title bar are *Customize*, and *Detach*.

- *Detach* moves the CLI Console widget into a pop-up window that you can resize and reposition. Select *Attach*. to move the widget back to the dashboard's page.
- *Customize* enables you to change the appearance of the console by selecting fonts and colors for the text and background.

Features

Figure 14: The *Features* widget



The *Features* widget displays a number of *Basic Features* and *Security Features* and whether or not each feature is currently enabled or disabled. Options for features that are disabled will not appear in the web-based manager.

For more information, see “Feature settings” on page 37.

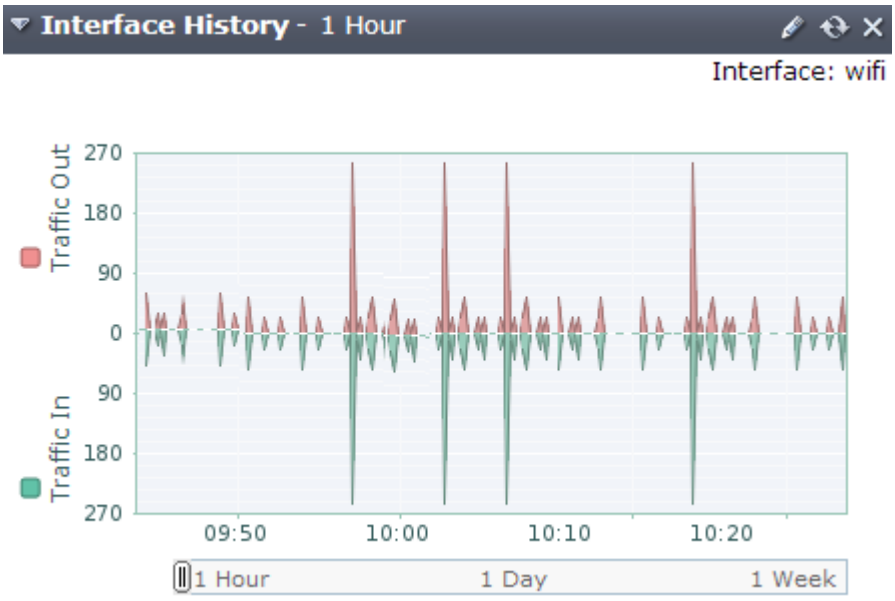
RAID monitor widget

The *RAID Monitor* widget displays the current state of the RAID array and each RAID disk. This widget does not display unless the FortiGate unit has more than one disk installed and is not available for FortiOS Carrier.

Array status icon	Displays the status of the RAID array. • Green with a check mark shows a healthy RAID array. • Yellow triangle shows the array is in a degraded state but it is still functioning. A degraded array is slower than a healthy array. Rebuild the array to fix the degraded state. • A wrench shows the array is being rebuilt. Positioning the mouse over the array status icon displays a text message of the status of the array.
Disk status icon	There is one icon for each disk in the array. • Green with a check mark shows a healthy disk. • Red with an X shows the disk has failed and needs attention. Positioning the mouse over the disk status icon displays the status of the disk, and the storage capacity of the disk.
RAID Level	The RAID level of this RAID array. The RAID level is set as part of configuring the RAID array.
Status bar	The bar shows the percentage of the RAID array that is currently in use.
Used/Free/Total	Displays the amount of RAID array storage that is being used, the amount of storage that is free, and the total storage in the RAID array. The values are in gigabytes.

Interface History

Figure 15: The *Interface History* widget

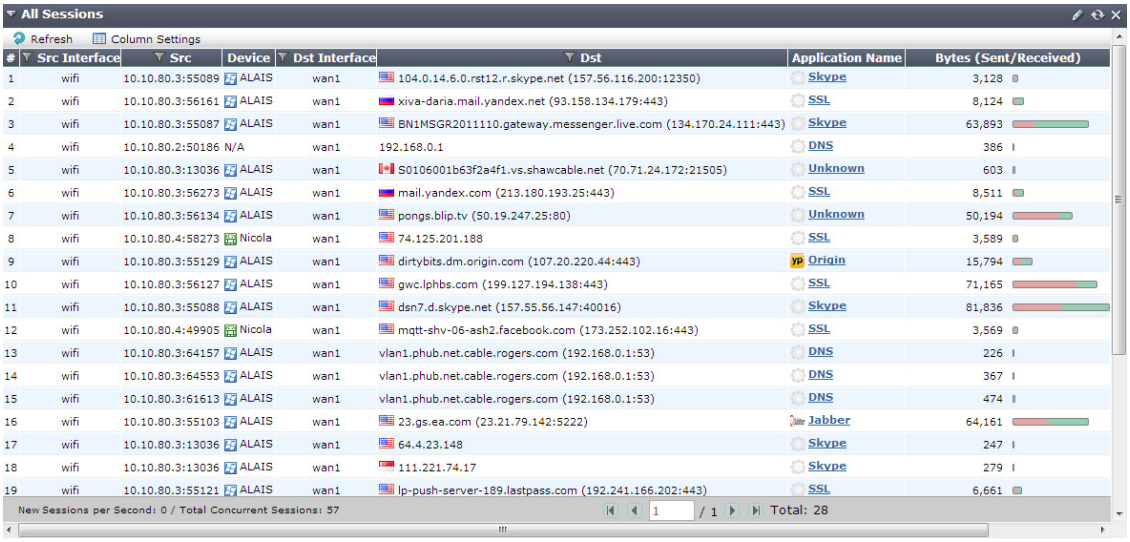


The *Interface History* widget displays the current activity and activity history of a system interface.

The current interface is visible in the top right-hand corner of the widget. You can change the interface that is shown by selecting the *Edit* icon and set *Select Network Interface* to the interface of your choice.

All Sessions

Figure 16: The *All Sessions* widget



The *All Sessions* widget shows information on your FortiGate's traffic. This widget can only be viewed on a dashboard that is set to have a one column display.

FortiView Dashboards

In order for information to appear in the *FortiView* dashboards, disk logging must be selected for the FortiGate unit. To select disk logging, go to *Log & Report* > *Log Config* > *Log Settings*.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

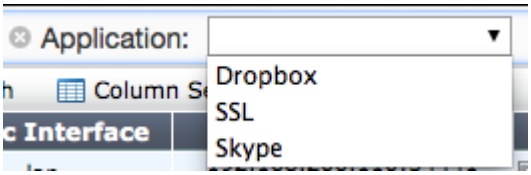
```
config log disk setting
  set status enable
end
```

Please note that flash-based logging has been disabled in FortiOS 5.2 for certain models. To view a complete list of affected models, please refer to the *Release Notes*.

The *FortiView* dashboards integrate real time and historical dashboards into a single view. These dashboards can be found by going to *Status* > *FortiView*. Each dashboard will initially display the top 100 sessions but when the results are filtered, other sessions may be displayed.

Each dashboards can be filtered by a variety of attributes. Attributes can be selected by using the dropdown menu located at the top of each widgets that displays only the options that have results; for example, if the only applications used in the are Dropbox, SSL, and Skype, the only options in the dropdown menu for the Application filter will be Dropbox, SSL, and Skype.

Figure 17: Filtering for Applications



Results can also be filtered using the various columns, although not all columns support this.

The dashboards also include different time options, allowing you to see current traffic in real-time, or historical traffic that occurred in the last 5 minutes, 1 hour, or 24 hours.

Historical traffic is only supported on FortiGate models that have local storage. The 24 hours option is also unavailable for desktop models (FortiGate-90 series and below).

Sources

The *Sources* dashboard shows information about the sources of traffic on your FortiGate unit, including user and device. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by source IP, source device, source interface, destination interface, and policy ID.

Figure 18: The *Sources* dashboard

Source	Device	Sessions	Bytes (Sent/Received)
10.10.80.3	Alais	122	539.94 K
10.10.80.4	Nicola	4	163.12 K
10.10.80.2	Wii	1	386

Applications

The *Applications* dashboard shows information about the applications being used on your network, including application name, category, and risk level. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the *Applications* dashboard, application control must be enabled in a policy.

Figure 19: The *Applications* dashboard

Application	Category	Risk	Sessions	Bytes (Sent/Received)
DNS	Network.Service		35	9.44 K
Skype	P2P		23	589.99 K
Hola.Unblocker	Proxy		21	440.08 K
SMTPS	Email		1	10.46 K
Dropbox	Storage.Backup		1	12.11 K

Cloud Applications

The *Cloud Applications* dashboard shows information about the cloud applications being used on your network, including application name, category, risk level, login IDs, and, if applicable, the number of videos played. If the cursor is held over the column showing the number of videos, the titles of these videos will be shown. Additional columns show information about sessions and bytes sent or received.

Two different views are available for the Cloud Applications dashboard: applications and users. Applications shows a list of the programs being used. Users shows information on the individual users of the cloud applications, including the username if the FortiGate was able to view the login event.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the *Cloud Applications* dashboard, an application control profile that has *Deep Inspection of Cloud Applications* turned on must be enabled in a policy and SSL Inspection must use `deep-inspection`.

Figure 20: The *Cloud Applications* dashboard

Application	Category	Risk	Login IDs	Sessions	Files (Up/Down)	Videos Played	Bytes (Sent/Receive
Youtube	Video/Audio		1	25		8	139.77 M
Vimeo	Video/Audio		1	1		1	4.85 M
Dropbox	File.Sharing		1	1	0 / 1		15.09 M

Destinations

The *Destinations* dashboard shows information about the destination IPs of traffic on your FortiGate unit, as well as the application used. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by destination IP, user, source interface, destination interface, and policy ID.

Figure 21: The *Destinations* dashboard

Destination	Applicati...	Sessions	Bytes (Sent/Received)
pongs.blip.tv (54.243.171.49)	Unknown	2	71.42 K
gwb.lphbs.com (199.127.194.181)	Unknown	1	45.33 K
notify3.dropbox.com (108.160.167.157)	Dropbox	1	555
dsn0.d.skype.net (157.55.130.156)	Unknown	1	8.29 K
dsn15.d.skype.net (157.55.56.154)	Unknown	1	3.84 K
104.0.14.6.0.rst6.r.skype.net (157.55.133.145)	Unknown	1	5.03 K

Web Sites

The *Web Sites* dashboard lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be clicked on in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand. New icons have also been added for FortiGuard category groups. Additional information is provided about domain, browsing time, threat weight, sources, and bytes sent or received.

This dashboard can be filtered by source interface, domain, destination interface, and policy ID.

In order for information to appear in the *Web Sites dashboard*, web filtering must be enabled in a policy, with FortiGuard Categories enabled.

Figure 22: The *Web Sites* dashboard

Filter Website Domains... | Domains | Categories | now | 5 minutes | 1 hour | 24 hours

Domain	Category	Browsing Time	Threat Weight	Sessions	Bytes (Sent/Received)
nytimes.com	News and Media	2h 3m 9s	0	491	143.70 M
www.bcit.ca	Unknown	12m 45s	0	84	22.90 M
nyt.com	Unknown	13m 24s	0	79	5.20 M
ubc.ca	Education	1h 17m 8s	0	65	3.71 M
moatads.com	Unknown	11m 38s	0	54	2.66 M
sfu.ca	Unknown	7m 16s	0	54	3.46 M
dynamicyield.com	Advertising	12m 1s	0	53	1.07 M
utoronto.ca	Unknown	14s	0	52	1.12 M
ubuntu.com	Reference	21s	0	44	19.59 M
google-analytics.com	Information Technology	1h 37m 38s	0	33	250.86 K
doubleclick.net	Advertising	13m 24s	0	32	467.48 K
cloudfront.net	Unknown	1h 18m 58s	0	31	1.30 M
flashtalking.com	Advertising	2m 32s	0	18	506.25 K
googlesyndication.com	Advertising	13m 24s	0	18	1.54 M
chartbeat.net	Information Technology	2m 21s	0	16	37.93 K
scorecardresearch.com	Business	13m 24s	0	16	215.78 K
krxd.net	Content Servers	10m 1s	0	15	51.83 K
revsci.net	Unknown	11m 38s	0	14	60.04 K
amazonaws.com	Unknown	18m 56s	0	12	622.93 K
fortinet.com	Information Technology	1m 8s	0	12	155.09 K
google.com	Freeware and Software Downloads	15h 26m 5s	0	11	121.19 K

Threats

The *Threats* dashboard lists the top users involved in incidents, as well as information on the top threats to your network. Additional information is provided about the threat, category, threat level, threat weight, and number of incidents.

This dashboard can be filtered by source interface, threat type, threat, destination interface, and policy ID.

In order for information to appear in the *Threats* dashboard, *Threat Weight Tracking* must be used.

Figure 23: The *Threats* dashboard

Threat	Category	Threat Le...	Threat Weight	Incidents
Failed Connection Attempts	Failed Connection Attempts	Medium	30	3

All Sessions

The *All Sessions* dashboard shows information about all FortiGate traffic. To choose which columns you wish to view, select *Column Settings* and place your desired columns in the right-hand box, in the order that you wish them to appear.

This dashboard can be filtered by source IP, destination IP, application, source device, source interface, destination interface, and policy ID. If you have set a filter in a different dashboard before viewing the *All Sessions* dashboard, that filter will remain until manually cleared.

Figure 24: The *All Sessions* dashboard

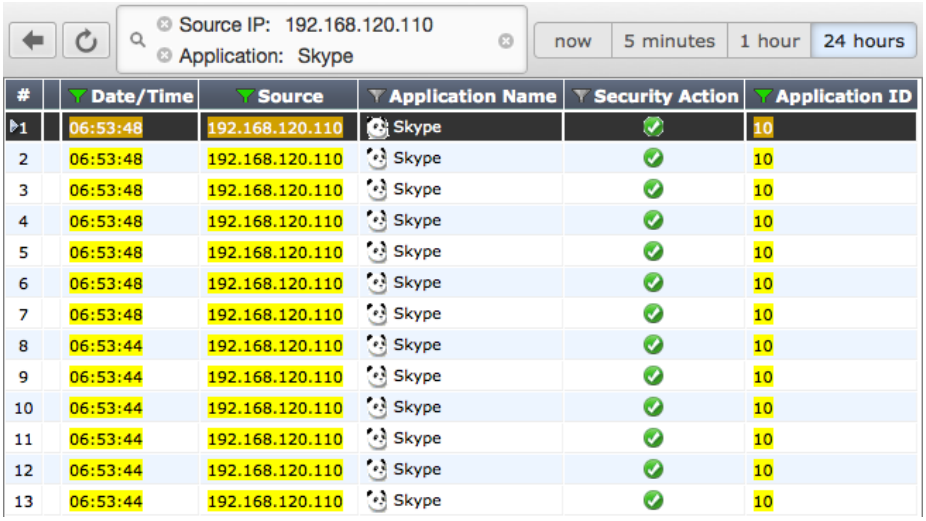
Time	Source	Destination	Application Name	Security Acti...	Threat	Sent /
	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown			4.11 KB /
	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown		AV EICAR_TEST_FILE	10.65 KB /
	192.168.120.110	38.127.167.7 (lastpass.com)	LastPass			2.02 KB /
	192.168.120.110	108.160.167.148 (d.dropbox.com)	Dropbox_Client.Sync			4.14 KB /
	192.168.120.110	134.170.24.141 (gateway.messenger.live.com)	Skype			10.75 KB /
	192.168.120.110	63.245.217.208 (phx-sync-13-2-8.services.mozilla.com)	SSL			8.66 KB /

Drilldown Options

In all FortiView dashboards except for the *All Sessions* dashboard, you can view more information about a particular session by right-clicking or double-clicking on the session to display the *Drilldown to details...* option, which opens a summary page that includes further information about applications, sources, destinations, and sessions where applicable.

From this summary page, you can access automatically filtered logs that will show a list of applicable sessions. For example, if you have picked the IP address 192.168.120.110 from the *Sources* dashboard, you can then select *Drilldown to details...* for Skype from the *Applications* column. This will open a log that displays all sessions from 192.168.1.1 that used Skype. From this page, you can select *Drilldown to details...* for any individual session, in order to view the log entry for that session.

Figure 25: Viewing Skype sessions from the Source Address 192.168.120.110



#	Date/Time	Source	Application Name	Security Action	Application ID
1	06:53:48	192.168.120.110	Skype	✓	10
2	06:53:48	192.168.120.110	Skype	✓	10
3	06:53:48	192.168.120.110	Skype	✓	10
4	06:53:48	192.168.120.110	Skype	✓	10
5	06:53:48	192.168.120.110	Skype	✓	10
6	06:53:48	192.168.120.110	Skype	✓	10
7	06:53:48	192.168.120.110	Skype	✓	10
8	06:53:44	192.168.120.110	Skype	✓	10
9	06:53:44	192.168.120.110	Skype	✓	10
10	06:53:44	192.168.120.110	Skype	✓	10
11	06:53:44	192.168.120.110	Skype	✓	10
12	06:53:44	192.168.120.110	Skype	✓	10
13	06:53:44	192.168.120.110	Skype	✓	10

In the *All Sessions* dashboard, filters are also used to narrow down what results are shown. If you are viewing historical traffic in the *All Sessions* dashboard, you can also add an element to a filter by right-clicking the element and selecting *Set Filter*.

Feature settings

Feature settings are used to disable features which are not required for network administration. Disabling features also removes all related configuration options from the web-based manager.

Some features are disabled by default and must be enabled in order to configure them using the web-based manager.

Enabling/disabling features

Feature Settings can be selected using the *Features* widget on the Status page, found at *System* > *Dashboard* > *Status*. When viewed in the Status Dashboard, the *Features* widget only displays a limited number of features. To view the entire list, select the *Edit* option for the widget.

Feature Settings can also be found at *System* > *Config* > *Features*, where additional features are also available by selecting *Show More*.

Once you have accessed Feature Settings, ensure all features you wish to use are turned on, while features you wish to hide are turned off. When you have finished, select *Apply*.

Security Features Presets

The main Security Features can be turned off individually or the five system presets can be used:

- **Full UTM** should be chosen for networks that require full protection from FortiOS. UTM is the default setting.
- **WF** should be chosen for networks that require web filtering.
- **ATP** should be chosen for networks that require protection from viruses and other external threats.
- **NGFW** should be chosen for networks that require application control and protection from external attacks.
- **NGFW + ATP** should be chosen for networks that require protection from external threats and attacks.

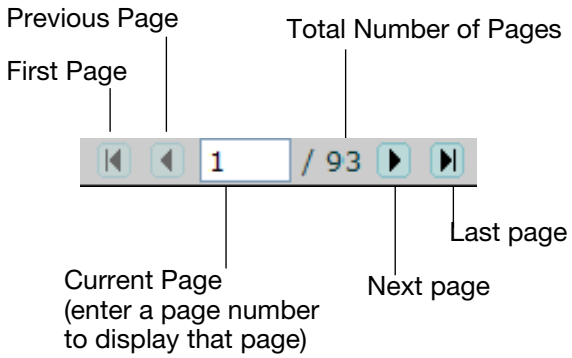
Information tables

Many of the web-based manager pages contain tables of information that you can filter to display specific information. Administrators with read and write access can define the filters.

Navigation

Some tables contain information and lists that span multiple pages. At the bottom of the page is the page navigation controls that enables you to move between pages.

Figure 26: Page controls



Adding filters to web-based manager lists

Filters are used to locate a specific set of information or content within multiple pages. These are especially useful in locating specific log entries. The specific filtering options vary, depending on the type of information in the log.

To create a filter, select *Filter Settings* or the filter icon in a column heading. When a filter is applied to a column, the filter icon becomes green. Filter settings are stored in the unit's configuration and will be maintained the next time that you access any list for which you have added filters.

Filtering variables can include: a numeric range (such as 25-50), an IP address or part of an address or any text string combination, including special characters.

Note that the filtering ignores characters following a "<" unless the followed by a space. For example, the filtering ignores `<string` but not `< string`. Filtering also ignores matched

opening and closing (< and >) characters and any characters between them. For example, filtering will ignore <string>.

For columns that contain only specific content, such as log message severity, a list of terms is provided from which options can be selected.

Using column settings

Column settings are used to select the types of information which are displayed on a certain page. Some pages have a large amounts of information is available and not all content can be displayed on a single screen. Also, some pages may contain content that is not of use to you. Using column settings, you can display only that content which is important to your requirements.

To configure column settings, right-click the header of a column and select the columns you wish to view and de-select any you wish to hide. After you have finished making your selections, select *Apply* (you may need to scroll down the list to do so).

Any changes that you make to the column settings of a list are stored in the unit's configuration and will display the next time that you access the list. To return a page's columns to their default state, select *Reset All Columns*, located at the bottom of the *Column Settings* menu.

Text strings

The configuration of a FortiGate unit is stored in the FortiOS configuration database. To change the configuration, you can use the web-based manager or CLI to add, delete, or change configuration settings. These changes are stored in the database as you make them.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable) settings.

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

Most web-based manager text string fields make it easy to add an acceptable number of characters and prevent you from adding the XSS vulnerability characters.

There is a different character limitation for VDOM names and hostnames. For both, the only legal characters are numbers (0-9), letters (a-z, A-Z), and special characters - and _.

From the CLI, you can also use the `tree` command to view the number of characters that are allowed in a name field. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager, you are limited to entering 64

characters in the firewall address name field. From the CLI you can enter the following `tree` command to confirm that the firewall address `name` field allows 64 characters.

```
config firewall address
  tree
  -- [address] --*name (64)
               |- subnet
               |- type
               |- start-ip
               |- end-ip
               |- fqdn (256)
               |- cache-ttl (0,86400)
               |- wildcard
               |- comment (64 xss)
               |- associated-interface (16)
               +- color (0,32)
```

The `tree` command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values set various sizes, rates, numeric addresses, and other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or, as in the case of MAC or IPv6 addresses, separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again, such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value fields make it easy to add the acceptable number of digits within the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

Basic Administration

This section contains information about basic FortiGate administration that can be done after you have installed the unit in your network.

While this section mainly focuses on tasks done using the web-based manager, some tasks include instructions to use the command line interface (CLI). You can connect to the CLI using the CLI Console widget, FortiExplorer, or by connecting using a SSH or Telnet connection. For more information about the CLI, see the *System Administration* handbook.

The following topics are included in this section:

- Registration
- System Settings
- Firmware
- FortiGuard
- FortiCloud
- Administrators
- Passwords
- Configuration Backups

Registration

In order to have full access to Fortinet Support and FortiGuard Services, you must register your FortiGate unit.

Registering your FortiGate:

1. Go to *System* > *Dashboard* > *Status* and locate the *License Information* widget.
2. Select *Register*.
3. A portal to the Fortinet Support site, https://support.fortinet.com, will open, allowing you to either sign in with an existing account and create a new one.
4. Once you have logged into the Support site, go to *Asset* > *Register/Renew* and use the *Registration Wizard* to register the FortiGate unit.

Once the FortiGate has been registered, the *License Information* widget will display the account and a *Launch Portal* option will appear, allowing you to open a portal to the Support site.

System Settings

There are several system settings that should be configured once your FortiGate is installed.

Default administrator password

By default, your FortiGate has an administrator account set up with the username `admin` and no password. In order to prevent unauthorized access to the FortiGate, it is highly recommended that you add a password to this account.

To change the default password:

1. Go to *System* > *Admin* > *Administrators*.
2. Edit the *admin* account.
3. Select *Change Password*.
4. Leave *Old Password* blank, enter the *New Password* and re-enter the password for confirmation.
5. Select *OK*.

For details on selecting a password and password best practices, see "Passwords" on page 73.

Language

The default language of the web-based manager is English. To change the language, go to *System* > *Admin* > *Settings*. In the *Display Settings* section, select the language you want from the *Language* drop-down list. For best results, you should select the language that is used by the management computer.

Time and date

For effective scheduling and logging, the FortiGate system date and time should be accurate. You can either manually set the system date and time or configure the FortiGate unit to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

The Network Time Protocol enables you to keep the FortiGate time in sync with other network systems. By enabling NTP on the FortiGate unit, FortiOS will check with the NTP server you select at the configured intervals. This will also ensure that logs and other time-sensitive settings on the FortiGate unit are correct.

The FortiGate unit maintains its internal clock using a built-in battery. At startup, the time reported by the FortiGate unit will indicate the hardware clock time, which may not be accurate. When using NTP, the system time might change after the FortiGate has successfully obtained the time from a configured NTP server.

By default, FortiOS has the daylight savings time configuration enabled. The system time must be manually adjusted after daylight saving time ends. To disable DST, enter the following command in the CLI:

```
config system global
   set dst disable
end
```

To set the date and time

1. Go to *System* > *Dashboard* > *Status* and locate the *System Information* widget.
2. Beside *System Time,* select *Change*.
3. Select your *Time Zone*.
4. Either select *Set Time* and manually set the system date and time, or select *Synchronize with NTP Server*. If you select synchronization, you can either use the default FortiGuard servers or specify a different server. You can also set the *Sync Interval*.
5. Select *OK*.

If you use an NTP server, you can identify a specific port/IP address for this self-originating traffic. The configuration is performed in the CLI with the command `set source-ip`. For

example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
  set ntpsyn enable
  set syncinterval 5
  set source-ip 192.168.4.5
end
```

Idle timeout

By default, the web-based manager disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the web-based manager if the management PC is left unattended.

To change the idle timeout

1. Go to *System* > *Admin* > *Settings*.
2. In the *Administration Settings* section, enter the time in minutes in the *Idle Timeout* field
3. Select *Apply*.

Administrator password retries and lockout time

By default, the FortiGate unit includes set number of three password retries, allowing the administrator a maximum of three attempts to log into their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts can be set to an alternate value, as well as the default wait time before the administrator can try to enter a password again. You can also change this to further sway would-be hackers. Both settings are must be configured with the CLI

To configure the lockout options:

```
config system global
  set admin-lockout-threshold <failed_attempts>
  set admin-lockout-duration <seconds>
end
```

For example, to set the lockout threshold to one attempt and a five minute duration before the administrator can try again to log in enter the commands”

```
config system global
  set admin-lockout-threshold 1
  set admin-lockout-duration 300
end
```

Administrative port settings

In order to improve security, you can change the default port configurations for administrative connections to the FortiGate. When connecting to the FortiGate unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiGate unit using port 99, the url would be `https://192.168.1.99:99`.

To configure the lockout options:

1. Go to *System* > *Admin* > *Settings*.

2. Under *Administrative Settings,* change the port numbers for HTTP, HTTPS, Telnet, and/or SSH as needed. You can also select *Redirect to HTTPS* in order to avoid HTTP being used for the administrators.

When you change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique. If a conflict exists with a particular port, a warning message will appear.

Changing the host name

The host name of your FortiGate unit appears in the *Host Name* row, in the *System Information* widget. The host name also appears at the CLI prompt when you are logged in to the CLI and as the SNMP system name.

To change the host name on the FortiGate unit, in the *System Information* widget, select *Change* in the *Host Name* row. The only administrators that can change a FortiGate unit's host name are administrators whose admin profiles permit system configuration write access. If the FortiGate unit is part of an HA cluster, you should use a unique host name to distinguish the FortiGate unit from others in the cluster.

RAID disk configuration

The RAID disk is configured from the Disk Configuration page.

RAID level	Select the level of RAID. Options include: • **RAID-0** — (striping) better performance, no redundancy • **RAID-1** — (mirroring) half the storage capacity, with redundancy • **RAID-5** — striping with parity checking, and redundancy Available RAID level options depend on the available number of hard disks. Two or more disks are required for RAID 0 or RAID 1. Three or more disks are required for RAID 5. Changing the RAID level will erase any stored log information on the array, and reboot the FortiGate unit. The FortiGate unit will remain offline while it reconfigures the RAID array. When it reboots, the array will need to synchronize before being fully operational.
Status	The status, or health, of RAID array. This status can be one of: • **OK** — standard status, everything is normal • **OK (Background-Synchronizing) (%)** — synchronizing the disks after changing RAID level, Synchronizing progress bar shows percent complete • **Degraded** — One or more of the disks in the array has failed, been removed, or is not working properly. A warning is displayed about the lack of redundancy in this state. Also, a degraded array is slower than a healthy array. Select *Rebuild RAID* to fix the array. • **Degraded (Background-Rebuilding) (%)** — The same as degraded, but the RAID array is being rebuilt in the background. The array continues to be in a fragile state until the rebuilding is completed.
Size	The size of the RAID array in gigabytes (GB). The size of the array depends on the RAID level selected, and the number of disks in the array.

Rebuild RAID	Select to rebuild the array after a new disk has been added to the array, or after a disk has been swapped in for a failed disk. If you try to rebuild a RAID array with too few disks you will get a rebuild error. After inserting a functioning disk, the rebuild will start. This button is only available when the RAID array is in a degraded state and has enough disks to be rebuilt. You cannot restart a rebuild once a rebuild is already in progress. **Note:** If a disk has failed, the number of working disks may not be enough for the RAID level to function. In this case, replace the failed disk with a working disk to rebuild the RAID array.
Disk#	The disk's position in the array. This corresponds to the physical slot of the disk. If a disk is removed from the FortiGate unit, the disk is marked as not a member of the array and its position is retained until a new disk is inserted in that drive bay.
Status	The status of this disk. Options include OK, and unavailable. A disk is unavailable if it is removed or has failed.

Firmware

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, https://support.fortinet.com.

Before you install any new firmware, be sure to follow the steps below:

- Review the *Release Notes* for a new firmware release.
- Review the *Supported Upgrade Paths* document to make sure the upgrade from your current image to the desired new image is supported.
- Backup the current configuration.
- Test the new firmware until you are satisfied that it applies to your configuration.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Backing up the current configuration

In case you need to restore your FortiGate configuration, you should always back up the configuration before installing new firmware.

To create a local back up:

1. Go to *System* > *Dashboard* > *Status* and locate the *System Information* widget.
2. Select *Backup* beside *System Configuration*.
3. Choose either *Local PC* or *USB Disk* to save the configuration file.
4. If desired, select *Encrypt configuration file*.
5. Select *Backup*.

Downloading firmware

Firmware images for all FortiGate units is available on the Fortinet Customer Support website, https://support.fortinet.com.

To download firmware

1. Log into the site using your user name and password.
2. Go to *Download* > *Firmware Images*.
3. A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware you wish to upgrade your FortiGate unit to.
4. Select *HTTPS Download*.

Firmware can also be downloaded using FTP; however, as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

5. Navigate to find the folder for the firmware version you wish to use.
6. Select your FortiGate model from the list. If your unit is a FortiWiFi, be sure to get the appropriate firmware, which will have a filename starting with FWF.
7. Save the firmware image to your computer.

Testing new firmware before installing

FortiOS enables you to test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure "Upgrading the firmware - web-based manager" on page 48.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 or null modem cable. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure, you must install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test the new firmware image

1. Connect to the CLI using a RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the FortiGate unit can connect to the TFTP server using the `execute ping` command.
5. Enter the following command to restart the FortiGate unit:

   ```
   execute reboot
   ```

6. As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages appears.
   When the following messages appears:

   ```
   Press any key to display configuration menu....
   ```

7. Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must login and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B[: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default
firmware.
[H]: Display this list of options.

Enter G, F, Q, or H:
```

8. Type G to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press Enter:

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address of the FortiGate unit to connect to the TFTP server.

    The IP address must be on the same network as the TFTP server.

Make sure you do not enter the IP address of another device on this network.

   The following message appears:

   ```
   Enter File Name [image.out]:
   ```

11. Enter the firmware image file name and press Enter.

    The TFTP server uploads the firmware image file to the FortiGate unit and the following appears.

    ```
    Save as Default firmware/Backup firmware/Run image without saving:
        [D/B/R]
    ```

12. Type `R`.

    The FortiGate image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.

You can test the new firmware image as required. When done testing, you can reboot the FortiGate unit, and the FortiGate unit will resume using the firmware that was running before you installed the test firmware.

Upgrading the firmware - web-based manager

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware

1. Log into the web-based manager as the admin administrative user.
2. Go to *System* > *Dashboard* > *Status* and locate the *System Information* widget.
3. Beside *Firmware Version*, select *Update*.
4. Type the path and filename of the firmware image file, or select *Browse* and locate the file.
5. Select *OK*.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

Upgrading the firmware - CLI

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For more information, see the *System Administration* handbook.

Before you begin, ensure you have a TFTP server running and accessible to the FortiGate unit.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware using the CLI

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the FortiGate unit can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   The FortiGate unit responds with the message:

```
This operation will replace the current firmware version!
     Do you want to continue? (y/n)
```

6. Type `y`.
7. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
8. Reconnect to the CLI.
9. Update antivirus and attack definitions, by entering:

   ```
   execute update-now
   ```

Installing firmware from a system reboot using the CLI

There is a possibility that the firmware upgrade does not load properly and the FortiGate unit will not boot, or continuously reboots. If this occurs, it is best to perform a fresh install of the firmware from a reboot using the CLI.

This procedure installs a firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9, or null modem cable. This procedure reverts the FortiGate unit to its factory default configuration.

For this procedure you install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure you back up the FortiGate unit configuration.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot

1. Connect to the CLI using the RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the internal interface is connected to the same network as the TFTP server.
5. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

6. Enter the following command to restart the FortiGate unit.

   ```
   execute reboot
   ```

   The FortiGate unit responds with the following message:

   ```
   This operation will reboot the system!
   Do you want to continue? (y/n)
   ```

7 Type `y`.

   As the FortiGate unit starts, a series of system startup messages appears. When the following messages appears:

   ```
   Press any key to display configuration menu.....
   ```

Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B[: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default
firmware.
[H]: Display this list of options.

Enter G, F, Q, or H:
```

8. Type G to get to the new firmware image form the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press Enter:

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address the FortiGate unit can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image filename and press Enter.

    The TFTP server uploads the firmware image file to the FortiGate unit and a message similar to the following appears:

    ```
    Save as Default firmware/Backup firmware/Run image without saving:
         [D/B/R]
    ```

12 Type `D`.

The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Reverting to a previous firmware version - web-based manager

The following procedures revert the FortiGate unit to its factory default configuration and deletes any configuration settings. If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Always remember to back up your configuration before making any changes to the firmware.

To revert to a previous firmware version

1. Go to *System* > *Dashboard* > *Status* and locate the *System Information widget*.
2. Beside *Firmware Version*, select *Update*.
3. Type the path and filename of the firmware image file, or select *Browse* and locate the file.
4. Select *OK*.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

Reverting to a previous firmware version - CLI

This procedure reverts the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure, it is recommended that you:

- back up the FortiGate unit system configuration using the command `execute backup config`
- back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- back up web content and email filtering lists

To use the following procedure, you must have a TFTP server the FortiGate unit can connect to.

To revert to a previous firmware version using the CLI

1. Make sure the TFTP server is running
2. Copy the firmware image file to the root directory of the TFTP server.
3. Log into the FortiGate CLI.
4. Make sure the FortiGate unit can connect to the TFTP server execute by using the `execute ping` command.

5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `imagev28.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image28.out 192.168.1.168
   ```

   The FortiGate unit responds with this message:

```
This operation will replace the current firmware version!
     Do you want to continue? (y/n)
```

6. Type `y`.

   The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following appears:

   ```
   Get image from tftp server OK.
        Check image OK.
        This operation will downgrade the current firmware version!
        Do you want to continue? (y/n)
   ```

7. Type `y`.
8. The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.
9. Reconnect to the CLI.
10. To restore your previous configuration, if needed, use the command:

    ```
    execute restore config <name_str> <tftp_ip4>
    ```

11. Update antivirus and attack definitions using the command:

    ```
    execute update-now.
    ```

Restore from a USB key - CLI

To restore configuration using the CLI

1. Log into the CLI.
2. Enter the following command to restore an unencrypted configuration file:

   ```
   exec restore image usb <filename>
   ```

   If your configuration file was encrypted, enter the following command:

   ```
   execute restore config usb-mode <password>
   ```

   The FortiGate unit responds with the following message:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```

3. Type `y`.

Configuration revision

The *Configuration Revisions* menu enables you to manage multiple versions of configuration files on models that have a 512 flash memory and higher. Revision control requires either a configured central management server or the local hard drive. The central management server can either be a FortiManager unit or FortiCloud.

If central management is not configured on your FortiGate unit, a message appears to tell you to do one of the following:

- enable central management
- obtain a valid license.

When revision control is enabled on your FortiGate unit, and configurations backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed in the *System Information* widget on the Dashboard.

Controlled upgrade

Using a controlled upgrade, you can upload a new version of the FortiOS firmware to a separate partition in the FortiGate memory for later upgrade. The FortiGate unit can also be configured so that when it is rebooted, it will automatically load the new firmware (CLI only). Using this option, you can stage a number of FortiGate units to do an upgrade simultaneously to all devices using FortiManager or script.

To load the firmware for later installation - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. Under *System Information* > *Firmware Version*, select *Update*.
3. Type the path and filename of the firmware image file, or select *Browse* and locate the file.
4. Deselect the *Boot the New Firmware* option
5. Select *OK*.

To load the firmware for later installation - CLI

```
execute restore secondary-image {ftp | tftp | usb}
```

To set the FortiGate unit so that when it reboots, the new firmware is loaded, use the CLI command...

```
execute set-next-reboot {primary | secondary}
```

... where `{primary | secondary}` is the partition with the preloaded firmware.

To trigger the upgrade using the web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. Under *System Information* > *Firmware Version*, select *Details.*
3. Select the check box for the new firmware version.

   The *Comments* column indicates which firmware version is the current active version.
4. Select *Upgrade* icon.

FortiGuard

The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.

The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging

threats.The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.

The FortiGuard services provide a number of services to monitor world-wide activity and provide the best possible security:

- **Intrusion Prevention System (IPS)**- The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats when no signature has yet been developed. It also provides more than 1000 application identity signatures for complete application control.
- **Application Control** - Application Control allows you to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources.
- **AntiVirus** -The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.
- **Web Filtering** - Web Filtering provides Web URL filtering to block access to harmful, inappropriate, and dangerous web sites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages - all continuously updated.
- **Vulnerability Scanning** - FortiGuard Services provide comprehensive and continuous updates for vulnerabilities, remediation, patch scan, and configuration benchmarks.
- **Email Filtering** - The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously via the FDN.
- **Messaging Services** - Messaging Services allow a secure email server to be automatically enabled on your FortiGate unit to send alert email or send email authentication tokens. With the SMS gateway, you can enter phone numbers where the FortiGate unit will send the SMS messages. Note that depending on your carrier, there may be a slight time delay on receiving messages.
- **DNS and DDNS** - The FortiGuard DNS and DDNS services provide an efficient method of DNS lookups once subscribed to the FortiGuard network. This is the default option. The FortiGate unit connects automatically to the FortiGuard DNS server. If you do not register, you need to configure an alternate DNS server.

  Configure the DDNS server settings using the CLI commands:

```
config system fortiguard
  set ddns-server-ip
  set ddns-server-port
end
```

Support Contract and FortiGuard Subscription Services

The *Support Contract* and *FortiGuard Subscription Services* sections are displayed in abbreviated form within the *License Information* widget. A detailed version is available by going to *System* > *Config* > *FortiGuard*.

The Support Contract area displays the availability or status of your FortiGate unit's support contract. The status displays can be either *Unreachable, Not Registered,* or *Valid Contract*.

The FortiGuard Subscription Services area displays detailed information about your FortiGate unit's support contract and FortiGuard subscription services. On this page, you can also manually update the antivirus and IPS engines.

The status icons for each section Indicates the state of the subscription service. The icon corresponds to the availability description.

- **Gray (Unreachable)** – the FortiGate unit is not able to connect to service.
- **Orange (Not Registered)** – the FortiGate unit can connect, but not subscribed.
- **Yellow (Expired)** – the FortiGate unit had a valid license that has expired.
- **Green (Valid license)** – the FortiGate unit can connect to FDN and has a registered support contract. If the Status icon is green, the expiry date also appears.

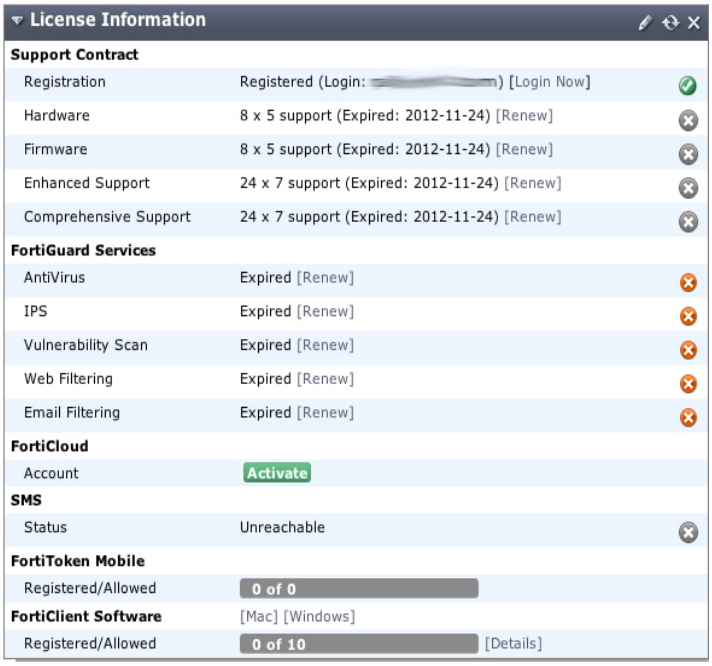
Verifying your Connection to FortiGuard

If you are not getting FortiGuard web filtering or antispam services, there are a few things to verify communication to the FortiGuard Distribution Network (FDN) is working. Before any troubleshooting, ensure that the FortiGate unit has been registered and you or your company, has subscribed to the FortiGuard services.

Verification - web-based manager

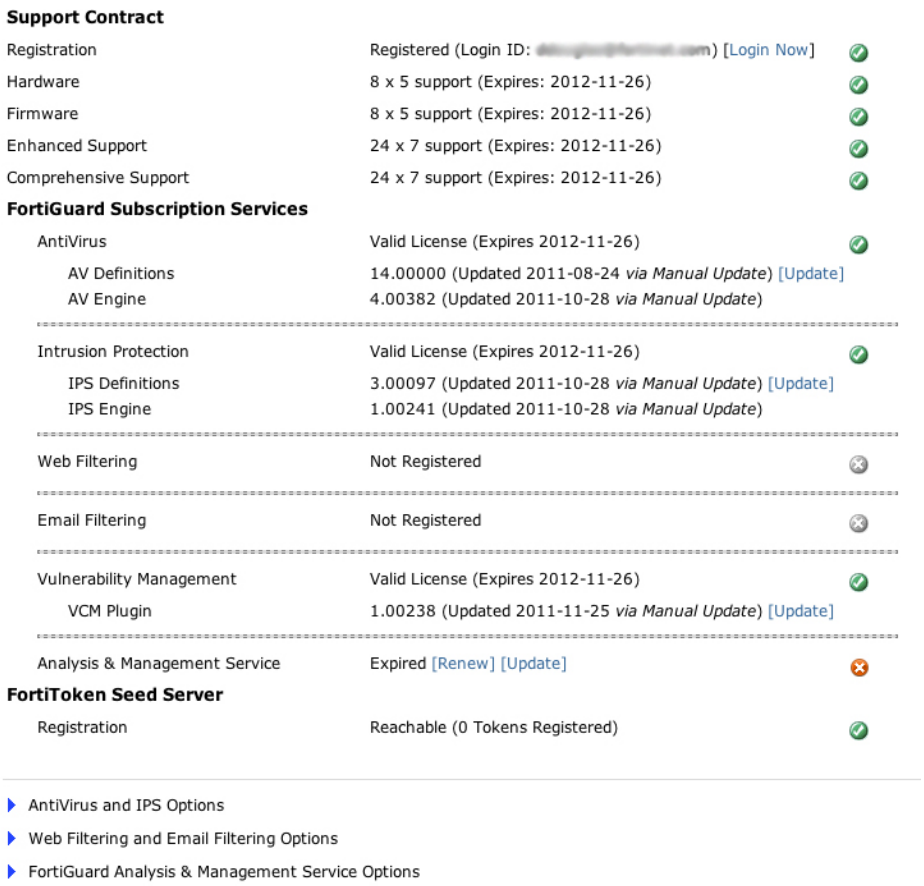
The simplest method to check that the FortiGate unit is communicating with the FDN, is to check the *License Information* dashboard widget. Any subscribed services should have a green check mark beside them indicating that connections are successful. Any other icon indicates a problem with the connection, or you are not subscribed to the FortiGuard services.

Figure 27: License Information widget showing FortiGuard availability



You can also view the FortiGuard connection status by going to *System* > *Config* > *FortiGuard*.

Figure 28: FortiGuard availability



Verification - CLI

You can also use the CLI to see what FortiGuard servers are available to your FortiGate unit. Use the following CLI command to ping the FDN for a connection:

```
ping guard.fortinet.net
```

You can also use diagnose command to find out what FortiGuard servers are available:

```
diagnose debug rating
```

From this command, you will see output similar to the following:

```
Locale       : english
License      : Contract
Expiration   : Sun Jul 24 20:00:00 2011
Hostname     : service.fortiguard.net

-=- Server List (Tue Nov  2 11:12:28 2010) -=-

IP Weight    RTT Flags  TZ    Packets  Curr Lost Total Lost
69.20.236.180 0     10        -5      77200          0          42
69.20.236.179 0     12        -5      52514          0          34
66.117.56.42 0     32        -5      34390          0          62
80.85.69.38 50    164         0      34430          0        11763
208.91.112.194 81    223 D      -8      42530          0        8129
216.156.209.26 286    241 DI     -8      55602          0      21555
```

An extensive list of servers are available. Should you see a list of three to five available servers, the FortiGuard servers are responding to DNS replies to service.FortiGuard.net, but the INIT requests are not reaching FDS services on the servers.

The rating flags indicate the server status:

D	Indicates the server was found via the DNS lookup of the hostname. If the hostname returns more than one IP address, all of them will be flagged with 'D' and will be used first for INIT requests before falling back to the other servers.
I	Indicates the server to which the last INIT request was sent
F	The server has not responded to requests and is considered to have failed.
T	The server is currently being timed.

The server list is sorted first by weight and then the server with the smallest RTT is put at the top of the list, regardless of weight. When a packet is lost, it will be resent to the next server in the list.

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a faraway server, the weight is not allowed to dip below a base weight, which is calculated as the difference in hours between the FortiGate unit and the server multiplied by 10. The further away the server is, the higher its base weight and the lower in the list it will appear.

Port assignment

FortiGate units contact the FortiGuard Distribution Network (FDN) for the latest list of FDN servers by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets have a destination port of 1027 or 1031.

If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets. As a result, the FortiGate unit will not receive the complete FDN server list.

If your ISP blocks the lower range of UDP ports (around 1024), you can configure your FortiGate unit to use higher-numbered ports, using the CLI command…

```
config system global
  set ip-src-port-range <start port>-<end port>
end
```

…where the `<start port>` and `<end port>` are numbers ranging of 1024 to 25000.

For example, you could configure the FortiGate unit to not use ports lower than 2048 or ports higher than the following range:

```
config system global
  set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use. Push updates might be unavailable if:

- there is a NAT device installed between the unit and the FDN
- your unit connects to the Internet using a proxy server.

FortiCloud is a hosted security management and log retention service for FortiGate products. It gives you a centralized reporting, traffic analysis, configuration and log retention without the need for additional hardware and software.

Configuring Antivirus and IPS Options

Go to *System* > *Config* > *FortiGuard*, and expand the *AV and IPS Options* section to configure the antivirus and IPS options for connecting and downloading definition files.

Use override server address	Select to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server.
Allow Push Update	Select to allow updates sent automatically to your FortiGate unit when they are available
Allow Push Update status icon	The status of the FortiGate unit for receiving push updates: • **Gray (Unreachable)** - the FortiGate unit is not able to connect to push update service • **Yellow (Not Available)** - the push update service is not available with your current support license • **Green (Available)** - the push update service is allowed.
Use override push IP and Port	Available only if both *Use override server address* and *Allow Push Update* are enabled. Enter the IP address and port of the NAT device in front of your FortiGate unit. FDS will connect to this device when attempting to reach the FortiGate unit. The NAT device must be configured to forward the FDS traffic to the FortiGate unit on UDP port 9443.
Schedule Updates	Select this check box to enable updates to be sent to your FortiGate unit at a specific time. For example, to minimize traffic lag times, you can schedule the update to occur on weekends or after work hours. Note that a schedule of once a week means any urgent updates will not be pushed until the scheduled time. However, if there is an urgent update required, select the *Update Now* button.
Update Now	Select to manually initiate an FDN update.
Submit attack characteristics… (recommended)	Select to help Fortinet maintain and improve IPS signatures. The information sent to the FortiGuard servers when an attack occurs and can be used to keep the database current as variants of attacks evolve.

Manual updates

To manually update the signature definitions file, you need to first go to the Support web site at https://support.fortinet.com. Once logged in, select FortiGuard Service Updates from the Download area of the web page. The browser will present you the most current antivirus and IPS signature definitions which you can download.

Once downloaded to your computer, log into the FortiGate unit to load the definition file.

To load the definition file onto the FortiGate unit

1. Go to *System* > *Config* > *FortiGuard*.
2. Select the *Update* link for either *AV Definitions or IPS Definitions*.
3. Locate the downloaded file and select *OK*.

The upload may take a few minutes to complete.

Automatic updates

The FortiGate unit can be configured to request updates from the FortiGuard Distribution Network. You can configure this to be on a scheduled basis, or with push notifications.

Scheduling updates

Scheduling updates ensures that the virus and IPS definitions are downloaded to your FortiGate unit on a regular basis, ensuring that you do not forget to check for the definition files yourself. As well, by scheduling updates during off-peak hours, such as evenings or weekends, when network usage is minimal, ensures that the network activity will not suffer from the added traffic of downloading the definition files.

If you require the most up-to-date definitions as viruses and intrusions are found in the wild, the FortiGuard Distribution Network can push updates to the FortiGate units as they are developed. This ensures that your network will be protected from any breakouts of a virus within the shortest amount of time, minimizing any damaging effect that can occur. Push updates require that you have registered your FortiGate unit.

Once push updates are enabled, the next time new antivirus or IPS attack definitions are released, the FDN notifies all the FortiGate unit that a new update is available. Within 60 seconds of receiving a push notification, the unit automatically requests the update from the FortiGuard servers.

To enable scheduled updates - web-based manager

1. Go to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *AV and IPS Options*.
3. Select the *Scheduled Update* check box.
4. Select the frequency of the updates and when within that frequency.
5. Select *Apply*.

To enable scheduled updates - CLI

```
config system autoupdate schedule
  set status enable
  set frequency {every | daily | weekly}
  set time <hh:mm>
  set day <day_of_week>
end
```

Push updates

Push updates enable you to get immediate updates when new virus or intrusions have been discovered and new signatures are created. This ensures that when the latest signature is available it will be sent to the FortiGate.

When a push notification occurs, the FortiGuard server sends a notice to the FortiGate unit that there is a new signature definition file available. The FortiGate unit then initiates a download of the definition file, similar to the scheduled update.

To ensure maximum security for your network, you should have a scheduled update as well as enable the push update, in case an urgent signature is created, and your cycle of the updates only occurs weekly.

To enable push updates - web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *AV and IPS Options*.
3. Select *Allow Push Update*.
4. Select *Apply*.

To enable push updates - CLI

```
config system autoupdate push-update
  set status enable
end
```

Push IP override

If the FortiGate unit is behind another NAT device (or another FortiGate unit), to ensure it receives the push update notifications, you need to use an override IP address for the notifications. To do this, you create a virtual IP to map to the external port of the NAT device.

Generally speaking, if there are two FortiGate devices as in the diagram below, the following steps need to be completed on the FortiGate NAT device to ensure the FortiGate unit on the internal network receives the updates:

- Add a port forwarding virtual IP to the FortiGate NAT device that connects to the Internet by going to *Firewall Objects* > *Virtual IP*.
- Add a security policy to the FortiGate NAT device that connects to the Internet that includes the port forwarding virtual IP.
- Configure the FortiGate unit on the internal network with an override push IP and port.

On the FortiGate internal device, the virtual IP is entered as the *Use push override IP* address.

To enable push update override- web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *AV and IPS Options*.
3. Select *Allow Push Update*.
4. Select *Use push override IP*.
5. Enter the virtual IP address configured on the NAT device.
6. Select *Apply*.

To enable push updates - CLI

```
config system autoupdate push-update
  set status enable
  set override enable
  set address <vip_address>
end
```

Configuring Web Filtering and Email Filtering Options

Go to *System* > *Config* > *FortiGuard*, and expand arrow to view *Web Filtering and Email Filtering Options* for setting the size of the caches and ports used.

Web Filter cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate unit will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate unit will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Antispam cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate unit will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate unit will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Port Section	Select the port assignments for contacting the FortiGuard servers. Select the *Test Availability* button to verify the connection using the selected port.
To have a URL's category rating re-evaluated, please click here	Select to re-evaluate a URL's category rating on the FortiGuard Web Filter service.

Email filtering

The FortiGuard data centers monitor and update email databases of known spam sources. With FortiGuard Antispam enabled, the FortiGate unit verifies incoming email sender address and IPs against the database, and take the necessary action as defined within the antivirus profiles.

Spam source IP addresses can also be cached locally on the FortiGate unit, providing a quicker response time, while easing load on the FortiGuard servers, aiding in a quicker response time for less common email address requests.

By default, the antispam cache is enabled. The cache includes a time-to-live value, which is the amount of time an email address will stay in the cache before expiring. You can change this value to shorten or extend the time between 300 and 86400 seconds.

To modify the antispam filter cache size - web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *Web Filtering and Email Filtering Options*.
3. Enter the TTL value for the *antispam cache*.
4. Select *Apply*.

To modify the web filter cache size - CLI

```
config system fortiguard
  set antispam-cache-ttl <integer>
end
```

Further antispam filtering options can be configured to block, allow or quarantine, specific email addresses. These configurations are available through the *Security Profiles* > *Antispam* menu. For more information, see the *Security Profiles handbook*.

Online Security Tools

The FortiGuard online center provides a number of online security tools that enable you to verify or check ratings of web sites, email addresses as well as check file for viruses:

- **URL lookup** - By entering a web site address, you can see if it has been rated and what category and classification it is filed as. If you find your web site or a site you commonly go to has been wrongly categorized, you can use this page to request that the site be re-evaluated.

  http://www.fortiguard.com/webfiltering/webfiltering.html

- **IP and signature lookup** - The IP and signature lookup enables you to check whether an IP address is blacklisted in the FortiGuard IP reputation database or whether a URL or email address is in the signature database.

  http://www.fortiguard.com/antispam/antispam.html

- **Online virus scanner** - If you discover a suspicious file on your machine, or suspect that a program you downloaded from the Internet might be malicious you can scan it using the FortiGuard online scanner. The questionable file can be uploaded from your computer to a dedicated server where it will be scanned using FortiClient Antivirus. Only one file of up to 1 MB can be checked at any one time. All files will be forwarded to our research labs for analysis.

  http://www.fortiguard.com/antivirus/virus_scanner.html

- **Malware removal tools** - Tools have been developed by FortiGuard Labs to disable and remove the specific malware and related variants. Some tools have been developed to remove specific malware, often tough to remove. A universal cleaning tool, FortiCleanup, is also available for download.

  The FortiCleanup is a tool developed to identify and cleanse systems of malicious rootkit files and their associated malware. Rootkits consist of code installed on a system with kernel level privileges, often used to hide malicious files, keylog and thwart detection / security techniques. The aim of this tool is to reduce the effectiveness of such malware by finding and eliminating rootkits. The tool offers a quick memory scan as well as a full system scan. FortiCleanup will not only remove malicious files, but also can cleanse registry entries, kernel module patches, and other tricks commonly used by rootkits - such as SSDT hooks and process enumeration hiding.

  A license to use these applications is provided free of charge, courtesy of Fortinet.

  http://www.fortiguard.com/antivirus/malware_removal.html

FortiCloud

FortiCloud (formerly known as FAMS) is a hosted security management and log retention service for FortiGate devices. It gives you centralized reporting, traffic analysis, configuration management and log retention without the need for additional hardware and software.

FortiGate models 800 and above do not support the FortiCloud service.

FortiCloud offers a wide range of features:

- **Simplified central management** - FortiCloud provides a central web-based management console to manage individual or aggregated FortiGate and FortiWiFi devices. Adding a

device to the FortiCloud management subscription is straightforward and provides detailed traffic and application visibility across the whole network.

- **Hosted log retention with large default storage allocated** - Log retention is an integral part of any security and compliance program but administering a separate storage system is burdensome. FortiCloud takes care of this automatically and stores the valuable log information in the cloud. Each device is allowed up to 200Gb of log retention storage. Different types of logs can be stored including Traffic, System Events, Web, Applications and Security Events.
- **Monitoring and alerting in real time** - Network availability is critical to a good end-user experience. FortiCloud enables you to monitor your FortiGate network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.
- **Customized or pre-configured reporting and analysis tools** - Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. For example, you may want to look closely at application usage or web site violations. The reports can be emailed as PDFs and can cover different time periods.
- **Maintain important configuration information uniformly** - The correct configuration of the devices within your network is essential to maintaining an optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.
- **Service security** - All communication (including log information) between the devices and the clouds is encrypted. Redundant data centers are always used to give the service high availability. Operational security measures have been put in place to make sure your data is secure — only you can view or retrieve it.

Registration and Activation

Before you can activate a FortiCloud account, you must first register your device.

FortiCloud accounts can be registered manually through the FortiCloud website, https://www.forticloud.com, but you can easily register and activate your account directly within your FortiGate unit. Your registration process will vary somewhat, depending on which firmware version and device you have.

FortiGate models 300 and below, all FortiWiFi units

1. On your device's dashboard, in the License Information widget, select the green *Activate* button in the FortiCloud section.
2. A dialogue asking you to register your FortiCloud account will appear. Enter your information, view and accept the Terms and Conditions and select *Create Account*.
3. A second dialogue window will appear, asking you to enter your information to confirm your account. This will send a confirmation email to your registered email. The dashboard widget will update to show that confirmation is required.
4. Open your email, and follow the confirmation link contained in it.

A FortiCloud page will open, stating that your account has been confirmed. The Activation Pending message on the dashboard will change to state the type of account you have ('1Gb Free' or '200Gb Subscription'), and will now provide a link to the FortiCloud portal.

FortiGate models 600 to 800

For 600 through 800, FortiCloud registration must be done through the FortiGate CLI Console.

Enabling logging to FortiCloud

1. Go to *Log & Report* > *Log Config* > *Log Settings*.
2. Enable *Send Logs to FortiCloud.*
3. Select *Test Connectivity* to ensure that your FortiGate can connect to the registered FortiCloud account.

Logging into the FortiCloud portal

Once logging has been configured and you have registered your account, you can log into the FortiCloud portal and begin viewing your logging results. There are two methods to reach the FortiCloud portal:

- If you have direct networked access to the FortiGate unit, you can simply open your Dashboard and check the License Information widget. Next to the current FortiCloud connection status will be a link to reach the FortiCloud Portal.
- If you do not currently have access to the FortiGate's interface, you can visit the FortiCloud website (https://forticloud.com) and log in remotely, using your email and password. It will ask you to confirm the FortiCloud account you are connecting to and then you will be granted access. Connected devices can be remotely configured using the Scripts page in the Management Tab, useful if an administrator may be away from the unit for a long period of time.

Upgrading to a 200Gb subscription

Upgrading your subscription is simple but must be done through the FortiGate unit, as the storage contract is allocated based on devices rather than user accounts.

1. Open the FortiGate Dashboard.
2. In the License Information widget, select *Upgrade* next to 'Type' in the FortiCloud section.
3. A new window will open, showing the Fortinet Support portal. Follow the on-screen instructions to register your contract.
4. Wait approximately 10 minutes for the contract to be applied and then visit your Dashboard.

In the License Information widget, Type will have changed from 'Free' to 'Subscribed'. Your maximum listed storage will also have updated.

Cloud Sandboxing

FortiCloud can be used for automated sample tracking, or sandboxing, for files from a FortiGate unit. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. This feature was formerly known as FortiGuard Analytics.

Cloud sandboxing is configured by going to *System* > *Config* > *FortiSandbox*. After enabling FortiSandbox, select *Cloud Sandbox (FortiCloud).*

Sandboxing results will be shown in a new tab called *AV Submissions* in the FortiCloud portal. This tab will only appear after a file has been sent for sandboxing.

Administrators

By default, the FortiGate unit has a super administrator called “admin”. This user login cannot be deleted and always has ultimate access over the FortiGate unit. Additional administrators can be added for various functions, each with a unique username, password, and set of access privileges.

There are two levels of administrator accounts; regular administrators and system administrators. Regular administrators are administrators with any admin profile other than the default super_admin. System administrators are administrators that are assigned the super_admin profile, which has the highest level of access.

Adding administrators

The name of the administrator should not contain the characters `<>()#"'`. Using these characters in the administrator account name can result in a cross site scripting (XSS) vulnerability.

Only the default ”admin” account or an administrator with read-write access control to add new administrator accounts and control their permission levels can create a new administrator account. If you log in with an administrator account that does not have the super_admin admin profile, the administrators list will show only the administrators for the current virtual domain.

When adding administrators, you are setting up the administrator’s user account. An administrator account comprises of an administrator’s basic settings as well as their access profile. The access profile is a definition of what the administrator is capable of viewing and editing.

To add an administrator - web-based manager

1. Go to *System* > *Admin* > *Administrators*.
2. Select *Create New*.
3. Enter the administrator name.
4. Select the type of account it will be. If you select *Remote*, the FortiGate unit can reference a RADIUS, LDAP or TACAS+ server.
5. When selecting *Remote* or *PKI* accounts, select the User Group the account will access.

   For information on logging in using remote authentication servers, see the *User Authentication Guide*. For an example of setting up a user with LDAP, see “LDAP Admin Access and Authorization” on page 66
6. Enter the password for the user.

   This may be a temporary password that the administrator can change later. Passwords can be up to 256 characters in length. For more information on passwords, see “Passwords” on page 73.
7. Select *OK*.

To add an administrator - CLI

```
config system admin
  edit <admin_name>
    set password <password>
    set accprofile <profile_name>
end
```

LDAP Admin Access and Authorization

You can use the LDAP server as a means to add administrative users, saving the time to add users to the FortiGate unit administrator list. After configuring, any user within the selected LDAP group server can automatically log into the FortiGate unit as an adm i st rat or. Ensure that the admin profile is the correct level of access, or the users within the LDAP group are the only ones authorized to configure or modify the configuration of the FortiGate unit.

To do this, requires three steps:

- configure the LDAP server
- add the LDAP server to a user group
- configure the administrator account

Configure the LDAP server

First set up the LDAP server as you normally would, and include a group to bind to.

To configure the LDAP server - web-based manager

1. Go to *User & Device* > *Remote* > *LDAP* and select *Create New*.
2. Enter a *Name* for the server.
3. Enter the *Server IP* address or name.
4. Enter the *Common Name Identifier* and *Distinguished Name*.
5. Set the *Bind Type to Regular* and enter the *User DN* and *Password*.
6. Select *OK*.

To configure the LDAP server - CLI

```
config user ldap
  edit <ldap_server_name>
    set server <server_ip>
    set cnid cn
    set dn DC=XYZ,DC=COM
    set type regular
    set username CN=Administrator,CN=Users,DC=XYZ,DC=COM
    set password <password>
    set member-attr <group_binding>
end
```

Add the LDAP server to a user group

Next, create a user group that will include the LDAP server that was created above.

To create a user group - web-based manager

1. Go to *User & Device* > *User Group* > *User Group* and select *Create New*.
2. Enter a *Name* for the group.
3. In the section labelled *Remote authentication servers*, select *Add*.
4. Select the *Remote Server* from the drop-down list.
5. Select *OK*.

To create a user group - CLI

```
config user group
  edit <group_name>
    config match
      edit 1
        set server-name <LDAP_server>
        set group-name <group_name>
    end
end
```

Configure the administrator account

Now you can create a new administrator, where rather than entering a password, you will use the new user group and the wildcard option for authentication.

To create an administrator - web-based manager

1. Go to *System* > *Admin* > *Administrators* and select *Create New*.
2. In the *Administrator* field, enter the name for the administrator.
3. For *Type*, select *Remote*.
4. Select the *User Group* created above from the drop-down list.
5. Select *Wildcard*.
6. The Wildcard option allows for LDAP users to connect as this administrator.
7. Select an *Admin Profile*.
8. Select *OK*.

To create an administrator - CLI

```
config system admin
  edit <admin_name>
    set remote-auth enable
    set accprofile super_admin
    set wildcard enable
    set remote-group ldap
end
```

Monitoring administrators

You can view the administrators logged in using the *System Information* widget on the Dashboard. On the widget is the *Current Administrator* row that shows the administrator logged in and the total logged in. Selecting *Details* displays the administrators), where they are logging in from and how (CLI, web-based manager) and when they logged in.

You are also able to monitor the activities the administrators perform on the FortiGate unit using the logging of events. Event logs include a number of options to track configuration changes.

To set logging - web-based manager

1. Go to *Log & Report* > *Log Config* > *Log Settings*.

2 Under *Event Logging*, ensure *System activity event* is selected.

3 Select *Apply*.

To set logging - CLI

```
config log eventfilter
  set event enable
  set system enable
end
```

To view the logs go to *Log & Report* > *Event Log*.

Administrator profiles

Administer profiles define what the administrator user can do when logged into the FortiGate unit. When you set up an administrator user account, you also assign an administrator profile, which dictates what the administrator user will see. Depending on the nature of the administrator's work, access level or seniority, you can allow them to view and configure as much, or as little, as required.

super_admin profile

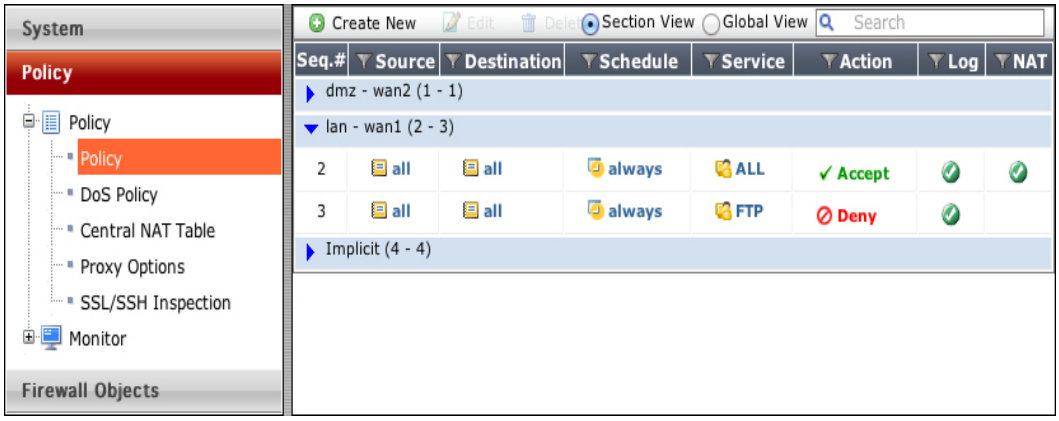
The super_admin administrator is the administrative account that the primary administrator should have to log into the FortiGate unit. The profile can not be deleted or modified to ensure there is always a method to administer the FortiGate unit.This user profile has access to all components of FortiOS, including the ability to add and remove other system administrators. For some administrative functions, such as backing up and restoring the configuration using SCP, super_admin access is required.

Creating profiles

To configure administrator profiles go to *System* > *Admin* > *Admin Profiles*. You can only assign one profile to an administrator user.

On the *New Admin Profile* page, you define the components of FortiOS that will be available to view and/or edit. For example, if you configure a profile so that the administrator can only access the firewall components, when an administrator with that profile logs into the FortiGate unit, they will only be able to view and edit any firewall components including policies, addresses, schedules and any other settings that directly affect security policies.

Figure 29: The view of an administrator with firewall-only access



Global and vdom profiles

By default, when you add a new administrative profile, it is set to have a vdom scope. That is, only the super_admin has a global profile that enables configuration of the entire FortiGate unit.

There may be instances where additional global administrative profiles may be required. To add more global profiles, use the following CLI command to set or change an administrative profile to be global.

```
config system accprofile
  set scope global
    ...
end
```

Once the scope is set, you can enable the read and read/write settings.

Regular (password) authentication for administrators

You can use a password stored on the local FortiGate unit to authenticate an administrator. When you select *Regular* for *Type*, you will see *Local* as the entry in the *Type* column when you view the list of administrators.

Management access

Management access defines how administrators are able to log on to the FortiGate unit to perform management tasks such as configuration and maintenance. Methods of access can include local access through the console connection or remote access over a network or modem interface using various protocols including Telnet and HTTPS.

You can configure management access on any interface in your VDOM. In NAT mode, the interface IP address is used for management access. In transparent mode, you configure a single management IP address that applies to all interfaces in your VDOM that permit management access. The FortiGate unit also uses this IP address to connect to the FDN for virus and attack updates.

The system administrator (admin) can access all VDOMs, and create regular administrator accounts. A regular administrator account can access only the VDOM to which it belongs and the management computer must connect to an interface in that VDOM. In both cases, the management computer must connect to an interface that permits management access and its IP address must be on the same network. Management access can be via HTTP, HTTPS, Telnet, or SSH sessions, if those services are enabled on the interface. HTTPS and SSH are preferred as they are more secure.

You can allow remote administration of the FortiGate unit. However, allowing remote administration from the Internet could compromise the security of the FortiGate unit. You should avoid this unless it is required for your configuration. The following precautions can be taken to improve the security of a FortiGate unit that allows remote administration from the Internet:

- Use secure administrative user passwords.
- Change these passwords regularly.
- Enable two-factor authentication for administrators.
- Enable secure administrative access to this interface using only HTTPS or SSH.
- Use Trusted Hosts to limit where the remote access can originate from.
- Do not change the system idle timeout from the default value of 5 minutes.

Security Precautions

One potential point of a security breach is at the management computer. Administrators who leave their workstations for a prolonged amount of time while staying logged into the web-based manager or CLI leave the firewall open to malicious intent.

Preventing unwanted login attempts

Setting trusted hosts for an administrator limits what computers an administrator can log in from, causing the FortiGate unit to only accept the administrator's login from the configured IP address. Any attempt to log in with the same credentials from any other IP address will be dropped.

Trusted hosts are configured when adding a new administrator by going to *System* > *Admin* > *Administrators* in the web-based manager or `config system admin` in the CLI.

To ensure the administrator has access from different locations, you can enter up to ten IP addresses, though ideally this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields. Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

The trusted hosts apply to the web-based manager, ping, SNMP, and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

Prevent multiple admin sessions

Multiple admin sessions can occur when multiple users access the FortiGate using the same admin account. By default, the FortiGate unit enables multiple logins of administrators using the same login credentials from different locations. To control admin log ins, and minimize the potential of configuration collisions, you can disable concurrent admin sessions. When disabled, only one user can use the admin account at a time. When a second admin attempts to connect, connection is denied with a message that the login attempt failed.

To disable concurrent admin sessions, enter the following command in the CLI:

```
config system global
  set admin-concurrent disable
end
```

On 2U FortiGate units, this option is also available in the Web-Based Manager by going to *System* > *Admin* > *Settings* and select *Allow each admin to log in with multiple sessions*.

Segregated administrative roles

To minimize the effect of an administrator causing errors to the FortiGate configuration and possibly jeopardizing the network, create individual administrative roles where none of the administrators have super-admin permissions. For example, one admin account is used solely to create security policies, another for users and groups, another for VPN, and so on.

Disable admin services

On untrusted networks, turn off the weak administrative services such as Telnet and HTTP. With these services, passwords are passed in the clear, not encrypted. These services can be disabled by going to *System* > *Network* > *Interface* and unselecting the required check boxes.

SSH login time out

When logging into the console using SSH, the default time of inactivity is 120 seconds (2 minutes) to successfully log into the FortiGate unit. To enhance security, you can configure the time to be shorter. Using the CLI, you can change the length of time the command prompt remains idle before the FortiGate unit will log the administrator out. The range can be between 10 and 3600 seconds.

To set the logout time enter the following commands:

```
config system global
  set admin-ssh-grace-time <number_of_seconds>
end
```

Idle time-out

To avoid the possibility of an administrator walking away from the management computer and leaving it exposed to unauthorized personnel, you can add an idle time-out that will automatically log the user out if the web-based manager is not used for a specified amount of time. This will cause the administrator to log in to the device again in order to continue their work.

The time-out can be set as high as 480 minutes, or eight hours, although this is not recommend.

To set the idle time out - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. In the *Administration Settings*, enter the amount of time the Administrator login can remain idol in the *Idle Timeout* field.
3. Select *Apply*.

To set the idle time out - CLI

```
config system global
  set admintimeout <minutes>
end
```

HTTPS redirect

When selecting port numbers for various protocols, you can also enable or disable the Redirect to HTTPS option. When enabled, if you select the Administrative Access for an interface to be only HTTP, HTTPS will automatically be enabled, allowing the administrator access with either HTTP or HTTPS. The administrator can then log in using HTTPS for better security.

Note that if an SSL VPN is also configured for the same port, the SSL connection is over the HTTPS protocol. In these situations, the FortiGate unit will not redirect an HTTP address to the SSL VPN HTTPS address. Ideally, the administrator should not have the management address and an SSL VPN portal on the same interface.

Log in/out warning message

For administrators logging in and out of the FortiGate unit, you can include a login disclaimer. This disclaimer provides a statement that must be accepted or declined where corporations are governed by strict usage policies for forensics and legal reasons.

The disclaimer is enabled through the CLI.

To disable an interface:

```
config system global
  set pre-login-banner enable
  set post-login-banner enable
end
```

When set, once the administrator enters their user name and password, the disclaimer appears. They must select either Accept or Decline to proceed. When the post login is enabled, once the administrator logs out they are presented with the same message.

The banner is a default message that you can customize by going to *System* > *Config* > *Replacement Messages*. Select *Extended View* to see the *Admin* category and messages.

Disable the console interface

To prevent any unwanted login attempts using the COM communication port, you can disable login connections to the FortiGate unit.

This command is specifically for the COM port. You can still use FortiExplorer to connect and configure the FortiGate unit if required.

To disable an interface:

```
config system console
  set login disable
end
```

Disable interfaces

If any of the interfaces on the FortiGate unit are not being used, disable traffic on that interface. This avoids someone plugging in network cables and potentially causing network bypass or loop issues.

To disable an interface - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select the interface from the list and select *Edit*.
3. For *Administrative Access*, select *Down*.
4. Select *OK*.

To disable an interface - CLI

```
config system interface
  edit <inerface_name>
    set status down
end
```

RADIUS authentication for administrators

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiGate units use the authentication and authorization functions of the RADIUS server. To use the RADIUS server for authentication, you must configure the server before configuring the FortiGate users or user groups that will need it.

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiGate unit sends the user's credentials to the RADIUS server for authentication. If the RADIUS server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the RADIUS server cannot authenticate the user, the FortiGate unit refuses the connection.

If you want to use a RADIUS server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the RADIUS server
- create the RADIUS user group
- configure an administrator to authenticate with a RADIUS server.

Configuring LDAP authentication for administrators

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, printers, etc.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. If the LDAP server cannot authenticate the administrator, the FortiGate unit refuses the connection.

If you want to use an LDAP server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure an LDAP server
- create an LDAP user group
- configure an administrator to authenticate with an LDAP server.

To view the LDAP server list, go to *User & Device* > *Remote* > *LDAP*.

For more information, see “LDAP Admin Access and Authorization” on page 66.

TACACS+ authentication for administrators

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiGate unit contacts the TACACS+ server for authentication. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiGate unit.

If you want to use an TACACS+ server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the TACACS+ server
- create a TACACS+ user group
- configure an administrator to authenticate with a TACACS+ server.

PKI certificate authentication for administrators

Public Key Infrastructure (PKI) authentication uses a certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Users only need a valid certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure a PKI user
- create a PKI user group
- configure an administrator to authenticate with a PKI certificate.

Passwords

Using secure admin passwords are vital for preventing unauthorized access to your FortiGate unit. When changing the password, consider the following to ensure better security:

- Do not make passwords that are obvious, such as the company name, administrator names, or other obvious word or phrase.
- Use numbers in place of letters, for example, `passw0rd`. Alternatively, spell words with extra letters, for example, *password*.
- Administrative passwords can be up to 64 characters.
- Include a mixture of letters, numbers, and upper and lower case.
- Use multiple words together, or possibly even a sentence, for example keytothehighway.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password, such as changing from `password` to `password1`.
- Write the password down and store it in a safe place away from the management computer, in case you forget it or ensure that at least two people know the password in the event that one person becomes ill, is away on vacation or leaves the company. Alternatively, have two different admin logins.

Password policy

The FortiGate unit includes the ability to enforce a password policy for administrator login. With this policy, you can enforce regular changes and specific criteria for a password including:

- minimum length between 8 and 64 characters.
- if the password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- if the password must contain numbers (1, 2, 3).
- if the password must contain non-alphanumeric characters (!, @, #, $, %, ^, &, *, ().
- where the password applies (admin or IPsec or both).
- the duration of the password before a new one must be specified.

To apply a password policy - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. Select *Enable Password Policy* and configure the settings as required.

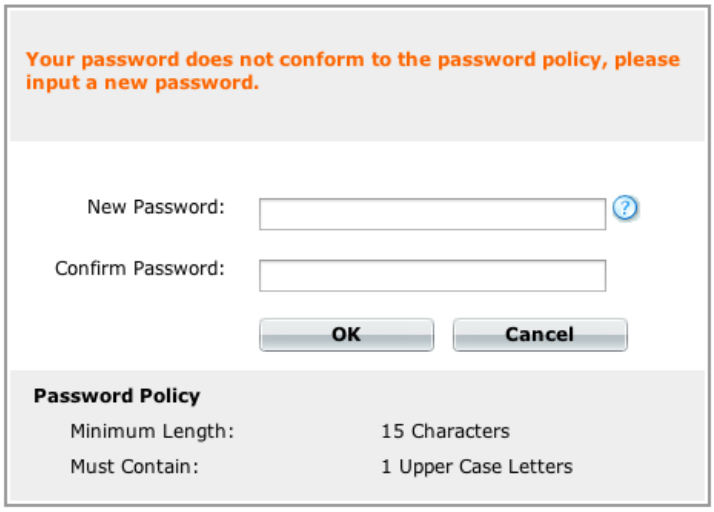
To apply a password policy - CLI

```
config system password-policy
  set status enable
```

Configure the other settings as required.

If you add a password policy or change the requirements on an existing policy, the next time that administrator logs into the FortiGate unit, they are prompted to update their password to meet the new requirements before proceeding to log in.

Figure 30: Password policy dialog box



Lost Passwords

If an administrator password has been lost, refer to the SysAdmin's Notebook article "Resetting a lost admin password," found at docs.fortinet.com/p/sysadmin-s-notebook-and-tech-notes.

Configuration Backups

Once you configure the FortiGate unit and it is working correctly, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate unit to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it.

It is also recommended that once *any* further changes are made that you backup the configuration immediately, to ensure you have the most current configuration available. Also, ensure you backup the configuration before upgrading the FortiGate unit's firmware. Should anything happen during the upgrade that changes the configuration, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site.The latter two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate unit or only a specific VDOM. Note that if you are using FortiManager or FortiCloud, full backups are performed and the option to backup individual VDOMs will not appear.

To back up the FortiGate configuration - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. On the *System Information* widget, select *Backup* for the *System Configuration*.
3. Select to backup to your *Local PC* or to a *USB key*.

   The *USB Disk* option will be grayed out if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
4. If VDOMs are enabled, select to backup the entire FortiGate configuration (*Full Config*) or only a specific VDOM configuration (*VDOM Config*).
5. If backing up a VDOM configuration, select the VDOM name from the list.

6. Select *Encrypt configuration file*.

   Encryption must be enabled on the backup file to back up VPN certificates.
7. Enter a password and enter it again to confirm it. You will need this password to restore the file.
8. Select *Backup*.
9. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

To back up the FortiGate configuration - CLI

```
execute backup config management-station <comment>
```

… or …

```
execute backup config usb <backup_filename> [<backup_password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>]
     [<user_name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_servers>
     <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
  edit <vdom_name>
```

Backup and restore a configuration file using SCP

You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. SCP is enabled using the CLI commands:

```
config system global
     set admin-scp enable
end
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config global
  set admin-scp enable
end
config vdom
  edit <vdom_name>
```

Enable SSH access on the interface

SCP uses the SSH protocol to provide secure file transfer. The interface you use for administration must allow SSH access.

To enable SSH - web-based manager:

1. Go to *System* > *Network* > *Interface*.
2. Select the interface you use for administrative access and select *Edit*.
3. In the *Administrative Access* section, select *SSH*.

4. Select *OK*.

To enable SSH - CLI:

```
config system interface
    edit <interface_name>
        set allowaccess ping https ssh
  end
```

When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

Using the SCP client

The FortiGate unit downloads the configuration file as `sys_conf`. Use the following syntax to download the file:

Linux

```
scp admin@<FortiGate_IP>:fgt-config <location>
```

Windows

```
pscp admin@<FortiGate_IP>:fgt-config <location>
```

The following examples show how to download the configuration file from a FortiGate-100D, at IP address 172.20.120.171, using Linux and Windows SCP clients.

Linux client example

To download the configuration file to a local directory called `~/config`, enter the following command:

```
scp admin@172.20.120.171:fgt-config ~/config
```

Enter the admin password when prompted.

Windows client example

To download the configuration file to a local directory called c:\config, enter the following command in a Command Prompt window:

```
pscp admin@172.20.120.171:fgt-config c:\config
```

Enter the admin password when prompted.

SCP public-private key authentication

SCP authenticates itself to the FortiGate unit in the same way as an administrator using SSH accesses the CLI. Instead of using a password, you can configure the SCP client and the FortiGate unit with a public-private key pair.

To configure public-private key authentication

1. Create a public-private key pair using a key generator compatible with your SCP client.

2. Save the private key to the location on your computer where your SSH keys are stored.

   This step depends on your SCP client. The Secure Shell key generator automatically stores the private key.

3. Copy the public key to the FortiGate unit using the CLI commands:

```
config system admin
    edit admin
        set ssh-public-key1 "<key-type> <key-value>"
    end
```

   <key-type> must be the ssh-dss for a DSA key or ssh-rsa for an RSA key. For the <key-value>, copy the public key data and paste it into the CLI command.

   If you are copying the key data from Windows Notepad, copy one line at a time and ensure that you paste each line of key data at the end of the previously pasted data. As well:

   - Do not copy the end-of-line characters that appear as small rectangles in Notepad.
   - Do not copy the `---- BEGIN SSH2 PUBLIC KEY ---- or Comment: "[2048-bit dsa,...]"` lines.
   - Do not copy the `---- END SSH2 PUBLIC KEY ----` line.

4 Type the closing quotation mark and press Enter.

Your SCP client can now authenticate to the FortiGate unit based on SSH keys rather than the administrator password.

Restoring a configuration using SCP

To restore the configuration using SCP, use the commands:

```
scp <local_file> <admin_user>@<FGT_IP>:fgt_restore_config
```

To use this command/method of restoring the FortiGate configuration, you need to log in as the "admin" administrator.

Restoring a configuration

Should you need to restore a configuration file, use the following steps:

To restore the FortiGate configuration - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. On the *System Information* widget, select *Restore* for the *System Configuration*.
3. Select to upload the configuration file to be restored from your *Local PC or a USB key*.

   The *USB Disk* option will be grayed out if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.

4. Enter the path and file name of the configuration file, or select *Browse* to locate the file.
5. Enter a password if required.
6. Select *Restore*.

To back up the FortiGate configuration - CLI

```
execute restore config management-station normal 0
```

… or …

```
execute restore config usb <filename> [<password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>]
     [<user_name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate unit will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Configuration revisions

The *Revisions* options on the *System Information* widget enables you to manage multiple versions of configuration files. Revision control requires either a configured central management server, or FortiGate units with 512 MB or more of memory. The central management server can either be a FortiManager unit or the FortiCloud.

When revision control is enabled on your unit, and configurations have been backed up, a list of saved revisions of those backed-up configurations appears.

Restore factory defaults

There may be a point where need to reset the FortiGate unit to its original defaults; for example, to begin with a fresh configuration. There are two options when restoring factory defaults. The first resets the entire device to the original out-of-the-box configuration:

To reset the FortiGate unit to its factory default settings - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. In the *System Information* widget, select *Restore* for the *System Configuration*.
3. Select *Restore Factory Defaults* at the top of the page.

You can reset using the CLI by entering the command:

```
execute factoryreset
```

When prompted, type `y` to confirm the reset.

Alternatively, in the CLI you can reset the factory defaults but retain the interface and VDOM configuration.

Use the command:

```
execute factoryreset2
```

Next Steps

Now that you have installed and set up your FortiGate unit, here's a list of some resources you can read next to help you continue to get the most out of your FortiGate.

Best Practices

The *Best Practices* document is a collection of guidelines to ensure the most secure and reliable operation of FortiGate units in a customer environment. It is updated periodically as new issues are identified.

This document can be found at http://docs.fortinet.com/d/fortigate-best-practices.

The FortiGate Cookbook

The *FortiGate Cookbook* contains a variety of step-by-step examples of how to integrate a FortiGate unit into your network and apply features such as security profiles, wireless networking, and VPN.

Using the Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

The FortiGate Cookbook can be found at http://docs.fortinet.com/fortigate/cookbook.

The Fortinet Video Library

The Fortinet Video Library contains video tutorials showing how to configure various Fortinet products, including FortiGate units. Many FortiGate videos are based on recipes from the FortiGate Cookbook.

The Fortinet Video Library can be found at http://video.fortinet.com.

The FortiOS Handbook

The *FortiOS Handbook* is the complete guide to FortiOS, covering a variety of FortiGate configurations.

The FortiOS Handbook is available as a single, complete document. Handbook chapters are also available as standalone documents.

The FortiOS Handbook can be found at http://docs.fortinet.com/fortigate/admin-guides.

Index